aws

Guia do Desenvolvedor

AWS Backup

AWS Backup: Guia do Desenvolvedor

Table of Contents

O que é AWS Backup?

AWS Backup é um serviço totalmente gerenciado que facilita a centralização e a automação da proteção de dados em todos os AWS serviços, na nuvem e no local. Usando esse serviço, você pode configurar políticas de backup e monitorar a atividade de seus AWS recursos em um só lugar. Ele permite automatizar e consolidar tarefas de backup que foram service-by-service executadas anteriormente e elimina a necessidade de criar scripts personalizados e processos manuais. Com alguns cliques no console do AWS Backup , é possível automatizar suas políticas e cronogramas de proteção de dados.

AWS Backup não rege os backups que você faz em seu AWS ambiente externo. AWS Backup Portanto, se você quiser uma end-to-end solução centralizada para os requisitos de conformidade comercial e regulatória, comece a usá-la AWS Backup hoje mesmo.

Visão geral do recurso

AWS Backup fornece muitos recursos e capacidades, incluindo os seguintes.

Gerenciamento centralizado de backups

AWS Backup fornece um console de backup centralizado, um conjunto de APIs de backup e o AWS Command Line Interface (AWS CLI) para gerenciar backups nos AWS serviços que seus aplicativos usam. Com AWS Backup, você pode gerenciar centralmente as políticas de backup que atendam aos seus requisitos de backup. Em seguida, você pode aplicá-las aos seus AWS recursos em todos AWS os serviços, permitindo que você faça backup dos dados do seu aplicativo de forma consistente e compatível. O console de backup AWS Backup centralizado oferece uma visão consolidada de seus backups e registros de atividades de backup, facilitando a auditoria de seus backups e garantindo a conformidade.

Backup baseado em políticas

Com AWS Backup, você pode criar políticas de backup conhecidas como planos de backup. Use esses planos de backup para definir seus requisitos de backup e depois aplicá-los aos AWS recursos que você deseja proteger nos AWS serviços que você usa. Você pode criar planos de backup diferentes que atendam aos requisitos específicos de conformidade regulamentar e empresarial. Isso ajuda a garantir que cada AWS recurso seja copiado de acordo com seus requisitos. Os planos de backup facilitam impor sua estratégia de backup em toda a sua organização e em seus aplicativos de modo dimensionável.

Para ver todas as opções de configuração dos planos de backup, consulte Opções de planos e configuração de backup.

Políticas de backup baseadas em tag

Você pode usar AWS Backup para aplicar planos de backup aos seus AWS recursos de várias maneiras, incluindo marcá-los. A marcação facilita a implementação de sua estratégia de backup em todos os seus aplicativos e garante que todos os seus AWS recursos sejam copiados e protegidos. AWS as tags são uma ótima maneira de organizar e classificar seus AWS recursos. A integração com AWS tags permite que você aplique rapidamente um plano de backup a um grupo de AWS recursos, para que eles sejam copiados de forma consistente e compatível.

Para conhecer todas as formas de atribuir seus recursos aos planos de backup, consulte Atribuir recursos a um plano de backup.

Políticas de gerenciamento de ciclo de vida

AWS Backup permite que você atenda aos requisitos de conformidade e, ao mesmo tempo, minimize os custos de armazenamento de backup armazenando os backups em um nível de armazenamento frio de baixo custo. Você pode configurar políticas de ciclo de vida que transferem automaticamente os backups de armazenamento "quente" para armazenamento "frio" de acordo com a programação que você definiu.

Para obter uma lista de recursos que podem ser transferidos para armazenamento frio, consulte Disponibilidade de recursos por recurso. Para ver as etapas para ativar o armazenamento refrigerado em seu plano de backup, consulte Ciclo de vida e níveis de armazenamento.

Backup entre regiões

Usando AWS Backup, você pode copiar backups para vários backups diferentes Regiões da AWS sob demanda ou automaticamente como parte de um plano de backup agendado. O backup entre regiões é particularmente valioso se você tiver requisitos de continuidade dos negócios ou de conformidade para armazenar backups a uma distância mínima de seus dados de produção. Para obter mais informações, consulte Criar cópias de backup entre Regiões da AWS.

Gerenciamento entre contas e backup entre contas

Você pode usar AWS Backup para gerenciar seus backups em toda Contas da AWS a sua AWS Organizationsestrutura. Com o gerenciamento entre contas, é possível usar automaticamente

políticas de backup para aplicar planos de backup nas Contas da AWS em sua organização. Isso torna a conformidade e a proteção de dados eficientes em escala e reduz despesas operacionais. Ele também ajuda a eliminar a duplicação manual de planos de backup em contas individuais. Para obter mais informações, consulte Gerenciar recursos do AWS Backup em várias Contas da AWS.

Você também pode copiar backups para vários Contas da AWS dentro de sua estrutura AWS Organizations de gerenciamento. Dessa forma, você pode “inserir” os backups em uma única conta do repositório e, em seguida, “distribuir” os backups para obter maior resiliência. Criar cópias de backup entre Contas da AWS.

Antes de usar os recursos de gerenciamento entre contas e de backup entre contas, é necessário ter uma estrutura de organização existente configurada no AWS Organizations. Uma unidade organizacional (OU) é um grupo de contas que podem ser gerenciadas como uma única entidade. AWS Organizations é uma lista de contas que podem ser agrupadas em unidades organizacionais e gerenciadas como uma única entidade.

Auditoria e geração de relatórios com o AWS Backup Audit Manager

AWS Backup O Audit Manager ajuda você a simplificar a governança de dados e o gerenciamento de conformidade de seus backups AWS. AWS Backup O Audit Manager fornece controles integrados e personalizáveis que você pode alinhar com seus requisitos organizacionais. Também é possível usar esses controles para rastrear automaticamente suas atividades e recursos de backup.

AWS Backup O Audit Manager pode ajudá-lo a localizar atividades e recursos específicos que ainda não estão em conformidade com os controles que você definiu. Ele também gera relatórios diários que podem ser usados para demonstrar evidências de conformidade com seus controles ao longo do tempo.

Para incluir sua conformidade de backup junto com sua postura geral de conformidade, você pode importar automaticamente as descobertas do AWS Backup Audit Manager para AWS Audit Manager.

Backups incrementais

AWS Backup armazena eficientemente seus backups periódicos de forma incremental. O primeiro backup de um recurso da AWS faz o backup de uma cópia completa dos seus dados. Para cada backup incremental sucessivo, somente as alterações em seus AWS recursos são copiadas. Os backups incrementais permitem que você se beneficie da proteção de dados de backups frequentes e, ao mesmo tempo, minimize os custos de armazenamento.

Para obter uma lista de quais recursos são compatíveis com backups incrementais, consulte Disponibilidade de recursos por recurso.

AWS Backup Gerenciamento completo

Alguns tipos de recursos oferecem suporte ao AWS Backup gerenciamento completo. Os benefícios do AWS Backup gerenciamento completo incluem:

- Criptografia independente. AWS Backup criptografa automaticamente seus backups com a chave KMS do seu AWS Backup cofre, em vez de usar a mesma chave de criptografia do seu recurso de origem. Isso aumenta suas camadas de defesa. Consulte Criptografia para backups em AWS Backup Para mais informações.
- Nomes do recurso da Amazon (ARNs) do **`awsbackup`**. Os ARNs de backup começam com `arn:aws:backup` em vez de `arn:aws:`*`source-resource`*. Isso permite criar políticas de acesso que se aplicam especificamente aos backups e não aos recursos de origem. Consulte Controle de acesso Para mais informações.
- Faturamento de backup centralizado e tags de alocação de custos do Explorador de custos. As cobranças AWS Backup (incluindo armazenamento, transferências de dados, restaurações e exclusão antecipada) aparecem em “Backup” em sua Amazon Web Services fatura, em vez de aparecerem em cada recurso suportado. Também é possível usar as tags de alocação de custos do Explorador de custos para rastrear e otimizar seus custos de backup. Consulte Medição, custos e cobrança Para mais informações.

Para ver quais tipos de recursos são elegíveis para AWS Backup gerenciamento completo, consulteDisponibilidade de recursos por recurso.

Monitoramento da atividade de backup

AWS Backup fornece um painel que simplifica a auditoria das atividades de backup e restauração em todos AWS os serviços. Com apenas alguns cliques no AWS Backup console, você pode ver o status das tarefas de backup recentes. Você também pode restaurar trabalhos em vários AWS serviços para garantir que seus AWS recursos estejam protegidos adequadamente.

AWS Backup integra-se com a Amazon CloudWatch e a Amazon EventBridge. CloudWatch permite rastrear métricas e criar alarmes. EventBridge permite que você visualize e monitore AWS Backup eventos. Para obter mais informações, consulte Monitorando AWS Backup eventos usando EventBridge e Monitorando AWS Backup métricas com CloudWatch.

AWS Backup integra-se com AWS CloudTrail. CloudTrail oferece uma visão consolidada dos registros de atividades de backup que agilizam e facilitam a auditoria de como seus recursos são copiados. AWS Backup também se integra ao Amazon Simple Notification Service (Amazon SNS), fornecendo notificações de atividades de backup, como quando um backup é bem-sucedido ou uma restauração é iniciada. Para obter mais informações, consulte Registro de chamadas de AWS Backup API com CloudTrail e uso do Amazon SNS para rastrear AWS Backup eventos.

Proteger seus dados em cofres de backup

O conteúdo de cada AWS Backup backup é imutável, o que significa que ninguém pode alterar esse conteúdo. AWS Backup protege ainda mais seus backups em cofres de backup, o que os separa com segurança de suas instâncias de origem. Por exemplo, seu cofre reterá os backups do Amazon EC2 e do Amazon EBS de acordo com a política de ciclo de vida que você escolher, mesmo se você excluir a instância de origem do Amazon EC2 e os volumes do Amazon EBS.

Os cofres de backup oferecem criptografia e políticas de acesso baseadas em recursos que permitem que você defina quem tem acesso aos seus backups. Você pode definir políticas de acesso para um cofre de backup que definem quem tem acesso aos backups no cofre e as ações que eles podem executar. Isso fornece uma maneira simples e segura de controlar o acesso aos seus backups em todos AWS os serviços. Para revisar AWS as políticas gerenciadas pelo cliente AWS Backup, consulte Políticas gerenciadas para AWS Backup.

Você pode usar o AWS Backup Vault Lock para impedir que qualquer pessoa (inclusive você) exclua backups ou altere o período de retenção. AWS Backup O Vault Lock ajuda você a aplicar um modelo write-once-read-many(WORM) e adicionar outra camada de defesa à sua defesa em profundidade. Para começar, consulte AWS Backup Vault Lock.

Compatibilidade com obrigações de conformidade

AWS Backup ajuda você a cumprir suas obrigações globais de conformidade. AWS Backup está no escopo dos seguintes programas de AWS conformidade:

- FedRAMP High
- RGPD
- SOC 1, 2 e 3
- PCI
- HIPAA
- e muito mais

Conceitos básicos

Para saber mais AWS Backup, recomendamos que você comece comComeçando com AWS Backup.

AWS Recursos e aplicativos compatíveis

A seguir estão AWS os recursos e aplicativos de terceiros que você pode fazer backup e restaurar usando AWS Backup. Para ter mais informações, consulte the section called “Disponibilidade de recursos”.

Serviço	Tipos de recursos compatíveis
Amazon Elastic Compute Cloud (Amazon EC2)	Instâncias do Amazon EC2 (exceto AMIs em armazenamento de instância)
Amazon Simple Storage Service (Amazon S3)	Dados do Amazon S3
Amazon Elastic Block Store (Amazon EBS)	Volumes do Amazon EBS
Amazon DynamoDB	Tabelas do Amazon DynamoDB
Amazon Relational Database Service (Amazon RDS)	Instâncias de banco de dados do Amazon RDS (incluindo todos os mecanismos de banco de dados); clusters Multi-AZ
Amazon Aurora	Clusters do Aurora
Amazon Elastic File System (Amazon EFS)	Sistemas de arquivos do Amazon EFS
FSx para Lustre	Sistemas de arquivos do FSx parar Lustre
FSx para Windows File Server	Sistemas de arquivos do FSx para Windows File Server

Serviço	Tipos de recursos compatíveis
Amazon FSx para ONTAP NetApp	Sistemas de arquivos do FSx para ONTAP
Amazon FSx para OpenZFS	Sistemas de arquivos do FSx para OpenZFS
AWS Storage Gateway (Gateway de volume)	AWS Storage Gateway volumes
Amazon DocumentDB	Clusters baseados em instâncias do Amazon DocumentDB
Amazon Neptune	Clusters do Amazon Neptune
Amazon Redshift	Clusters do Amazon Redshift
Amazon Timestream	Tabelas Amazon Timestream
VMware Cloud™ ativado AWS	Máquinas virtuais VMware Cloud™ em AWS
VMware Cloud™ ativado AWS Outposts	Máquinas virtuais VMware Cloud™ em AWS Outposts
AWS CloudFormation	AWS CloudFormation pilhas
Bancos de dados SAP HANA	Bancos de dados SAP HANA nas instâncias do Amazon EC2

Definição de preço

Com AWS Backup, você paga pelo armazenamento de backup, pelos dados restaurados, pelos testes de restauração, pela transferência de dados entre regiões e pelo AWS Backup Audit Manager. Para obter mais informações, consulte Preços do AWS Backup.

AWS Backup disponibilidade de recursos

AWS Backup os recursos são oferecidos de acordo com o recurso Região da AWS e. As seções e tabelas a seguir podem ajudar você a determinar a disponibilidade dos recursos.

Conteúdo

Recursos disponíveis para todos os recursos compatíveis

AWS Backup oferece os seguintes recursos para seus AWS serviços suportados, bem como para aplicativos de terceiros compatíveis. A compatibilidade de um recurso ou serviço não deve ser presumida, a menos que seja explicitamente mencionada.

- Programações automatizadas de backup e gerenciamento de retenção
- Monitoramento centralizado de backup
- Backups criptografados
- Backups incrementais
- Gerenciamento de várias contas com AWS Organizations
- Auditorias e relatórios de backup automatizados com o AWS Backup Audit Manager
- Escreva uma vez, leia muitas (WORM) com o Vault Lock AWS Backup

Disponibilidade de recursos por recurso

Para usar AWS Backup com um AWS serviço compatível em uma região específica, o serviço deve estar disponível na região. Para determinar a disponibilidade do serviço em uma região, visualize os endpoints do serviço no Referência geral da AWS.

AWS Backup suporta	Backup entre regiões	Backup entre contas	AWS Backup Audit Manager	Backups incremen ais	Backup e point-in-time restaura ão contínuo	Gerencia ento completo	Ciclo de vida até o armazen ento refrigera do	Restauraç ão em nível de item 1	Teste de restauraç ão
Amazon EC2	✓	✓	✓	✓					✓
Amazon S3	✓	✓	✓	✓	✓	✓		✓	✓
Amazon EBS	✓	✓	✓	✓			✓		✓
Instância única do Amazon RDS	✓ [3]	✓ [3]	✓ [4]	✓	✓				✓
Cluster do Amazon RDS	✓ [3]	✓ [3]	✓ [4]	✓					✓
Amazon Aurora	✓ [3]	✓ [3]	✓	✓ [6]	✓				✓
Amazon EFS	✓	✓	✓	✓		✓	✓	✓	✓
FSx for Lustre	✓	✓	✓	✓					✓

AWS Backup suporta	Backup entre regiões	Backup entre contas	AWS Backup Audit Manager	Backups incremen ais	Backup e point-in-time restaura ão contínuo	Gerencia ento completo	Ciclo de vida até o armazen ento refrigera do	Restauraç ão em nível de item 1	Teste de restauraç ão
FSx for Windows File Server	✓	✓	✓	✓					✓
FSx para ONTAP			✓ [2]	✓					✓
FSx para OpenZF	✓	✓	✓	✓					✓
AWS Storage Gateway	✓	✓	✓	✓					
Amazon Docume B	✓ [3]	✓ [3]	✓						✓
Amazon Neptune	✓ [3]	✓ [3]	✓						✓
Amazon Redshift								✓	

AWS Backup suporta	Backup entre regiões	Backup entre contas	AWS Backup Audit Manager	Backups incremen ais	Backup e point-in-time restaura ão contínuo	Gerencia ento completo	Ciclo de vida até o armazen ento refrigera do	Restauraç ão em nível de item 1	Teste de restauraç ão
Timestre m	✓	✓	✓	✓		✓	✓	✓	
VSS do Windows	✓	✓	✓	✓					
Máquina virtuais	✓	✓	✓	✓		✓	✓	✓	
AWS CloudFo ation modelos	✓	✓		✓ [5]		✓	✓ [5]		
Amazon Dynamol			✓						✓
Dynamol com recursos avançad do AWS Backup	✓	✓	✓			✓	✓		✓

AWS Backup suporta	Backup entre regiões	Backup entre contas	AWS Backup Audit Manager	Backups incrementais	Backup e point-in-time restauração contínuo	Gerenciamento completo	Ciclo de vida até o armazenamento refrigerado	Restauração em nível de item 1	Teste de restauração
Bancos de dados SAP HANA nas instâncias do Amazon EC2				✓	✓	✓	✓		

Alguns tipos de recursos têm capacidade de backup contínuo e cópia entre regiões e entre contas. Quando uma cópia entre regiões ou entre contas de um backup contínuo é feita, o ponto de recuperação copiado (backup) se torna um backup de snapshot (periódico). O Amazon RDS e o Amazon S3 oferecem suporte a cópias incrementais de instantâneos; o Amazon Aurora oferece suporte somente a cópias completas de instantâneos. A PITR (para um ponto no tempo) não está disponível para essas cópias.

[1] O “item” em uma restauração em nível de item varia de acordo com o recurso suportado. Por exemplo, um item do sistema de arquivos é um arquivo ou diretório, enquanto um item do S3 é um objeto do S3. Um item da VMware é um disco. Para obter mais informações, consulte a seção Restaurar um backup do recurso compatível.

[2] O AWS Backup Audit Manager oferece suporte a esse recurso em todos os controles, exceto na cópia entre contas e na cópia entre regiões.

[3] RDS, Aurora, DocumentDB e Neptune não oferecem suporte a uma única ação de cópia que realize backup entre regiões e entre contas. É preciso escolher um ou outro. Você também pode usar

um AWS Lambda script para ouvir a conclusão da primeira cópia, executar a segunda cópia e excluir a primeira cópia. As instâncias de banco de dados do RDS com várias zonas de disponibilidade (Multi-AZ) podem ser copiadas, mas os clusters Multi-AZ não são compatíveis com a cópia entre regiões ou entre contas no momento. Consulte Considerações sobre cópia entre regiões com recursos específicos para obter mais informações.

[4] Consulte Backups de zona de multidisponibilidade do RDS para regiões onde o suporte do Backup Audit Manager está disponível.

[5] Nos backups em CloudFormation pilha, os recursos aninhados mantêm as características dos recursos de origem. No entanto, os recursos dentro da pilha não mantêm a funcionalidade Point-in-Time Restore (PITR) (como Amazon S3 e Amazon RDS). As propriedades na matriz acima se aplicam apenas aos CloudFormation modelos e não aos recursos na pilha.

[6] Para o Aurora, os instantâneos estão completos e o backup incremental é oferecido por meio da PITR.

Disponibilidade de recursos por Região da AWS

AWS Backup está disponível em todos os itens a seguir Regiões da AWS. AWS Backup os recursos estão disponíveis em todas essas regiões, salvo indicação em contrário na tabela a seguir.

AWS Backup suporta	Backup entre regiões	Gerenciamento entre contas	Backup entre contas	AWS Backup Painel do Audit Manager and Jobs	Teste de restauração
Leste dos EUA (Norte da Virgínia)	✓	✓	✓	✓	✓
Leste dos EUA (Ohio)	✓	✓	✓	✓	✓
Oeste dos EUA (N. da Califórnia)	✓	✓	✓	✓	✓

AWS Backup suporta	Backup entre regiões	Gerenciamento entre contas	Backup entre contas	AWS Backup Painel do Audit Manager and Jobs	Teste de restauração
Oeste dos EUA (Oregon)	✓	✓	✓	✓	✓
África (Cidade do Cabo)	✓		✓	✓	✓
Ásia-Pacífico (Hong Kong)	✓		✓	✓	✓
Ásia-Pacífico (Hyderabad)	✓		✓		✓
Ásia-Pacífico (Jacarta)	✓		✓		✓
Ásia-Pacífico (Melbourne)	✓		✓		✓
Ásia-Pacífico (Mumbai)	✓	✓	✓	✓	✓
Ásia-Pacífico (Osaka)	✓	✓	✓		✓
Ásia-Pacífico (Seul)	✓	✓	✓	✓	✓
Ásia-Pacífico (Singapura)	✓	✓	✓	✓	✓

AWS Backup suporta	Backup entre regiões	Gerenciamento entre contas	Backup entre contas	AWS Backup Painel do Audit Manager and Jobs	Teste de restauração
Ásia-Pacífico (Sydney)	✓	✓	✓	✓	✓
Ásia-Pacífico (Tóquio)	✓	✓	✓	✓	✓
Canadá (Central)	✓	✓	✓	✓	✓
Oeste do Canadá (Calgary)	✓ (exceto Amazon S3)		✓		
China (Pequim)	✓				
China (Ningxia)	✓				
Europa (Frankfurt)	✓	✓	✓	✓	✓
Europa (Irlanda)	✓	✓	✓	✓	✓
Europa (Londres)	✓	✓	✓	✓	✓
Europa (Milão)	✓		✓	✓	✓
Europe (Paris)	✓	✓	✓	✓	✓

AWS Backup suporta	Backup entre regiões	Gerenciamento entre contas	Backup entre contas	AWS Backup Painel do Audit Manager and Jobs	Teste de restauração
Europa (Espanha)	✓		✓		✓
Europa (Estocolmo)	✓	✓	✓	✓	✓
Europa (Zurique)	✓		✓		✓
Israel (Tel Aviv)	✓		✓		
Oriente Médio (Barém)	✓		✓	✓	✓
Oriente Médio (Emirados Árabes Unidos)	✓		✓		✓
América do Sul (São Paulo)	✓	✓	✓	✓	✓
AWS GovCloud (Leste dos EUA)	✓	✓	✓	✓	

AWS Backup suporta	Backup entre regiões	Gerenciamento entre contas	Backup entre contas	AWS Backup Painel do Audit Manager and Jobs	Teste de restauração
AWS GovCloud (Oeste dos EUA)	✓	✓	✓	✓	

China (Pequim) e China (Ningxia) são compatíveis com a cópia entre regiões de uma dessas duas regiões para a outra. Não há compatibilidade com a cópia entre regiões dessas regiões para outras regiões ou para essas regiões. Não há compatibilidade com a cópia entre contas nessas regiões.

O painel de empregos não está disponível em AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA). A agregação do painel de tarefas só está disponível em regiões que oferecem suporte ao gerenciamento de várias contas e ao AWS Backup Audit Manager.

O Amazon FSx para Windows File Server e o Amazon Neptune não oferecem suporte a cópias de backup entre regiões em regiões opcionais.

Serviços suportados por Região da AWS

AWS Backup suporta o seguinte em todas as regiões suportadas:

- Aurora
- DynamoDB
- DynamoDB AWS Backup com recursos avançados
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

A tabela a seguir indica AWS Backup suporte para outros Serviços da AWS por região.

Região e serviço	Amazon FSx	SAP HANA em instâncias do EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware e gateway de Backup
Leste dos EUA (Norte da Virgínia)	✓	✓	✓	✓	✓	✓
Leste dos EUA (Ohio)	✓	✓	✓	✓	✓	✓
Oeste dos EUA (N. da Califórnia)	Windows; Lustre; ONTAP	✓	✓	✓		✓
Oeste dos EUA (Oregon)	Windows; Lustre; ONTAP	✓	✓	✓	✓	✓
África (Cidade do Cabo)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Ásia-Pacífico (Hong Kong)	✓	✓	✓ [1]	✓		✓
Ásia-Pacífico (Hyderabad)	Windows; Lustre; ONTAP		✓ [1]	✓		
Ásia-Pacífico (Jacarta)	Windows; Lustre; ONTAP		✓	✓		

Região e serviço	Amazon FSx	SAP HANA em instâncias do EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware e gateway de Backup
Ásia-Pacífico (Melbourne)	Windows; Lustre; ONTAP		✓ [1]	✓		
Ásia-Pacífico (Mumbai)	✓	✓	✓	✓		✓
Ásia-Pacífico (Osaka)	Windows; Lustre	✓	✓ [1]	✓		✓
Ásia-Pacífico (Seul)	✓	✓	✓	✓		✓
Ásia-Pacífico (Singapura)	✓	✓	✓	✓		✓
Ásia-Pacífico (Sydney)	✓	✓	✓	✓	✓	✓
Ásia-Pacífico (Tóquio)	✓	✓	✓	✓	✓	✓
Canadá (Central)	✓	✓	✓	✓		✓

Região e serviço	Amazon FSx	SAP HANA em instâncias do EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware e gateway de Backup
Oeste do Canadá (Calgary)						
China (Pequim)	Windows; Lustre		✓ [1]	✓	✓	
China (Ningxia)	Windows; Lustre		✓ [1]	✓	✓	
Europa (Frankfurt)	✓	✓	✓	✓	✓	✓
Europa (Irlanda)	✓	✓	✓	✓	✓	✓
Europa (Londres)	✓	✓	✓	✓		✓
Europa (Milão)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Europa (Paris)	Windows; Lustre; ONTAP	✓	✓	✓		✓
Europa (Espanha)	Windows; Lustre; ONTAP		✓ [1]	✓		
Europa (Estocolmo)	✓	✓	✓	✓		✓

Região e serviço	Amazon FSx	SAP HANA em instâncias do EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware e gateway de Backup
Europa (Zurique)	Windows; Lustre; ONTAP		✓ [1]	✓		
Israel (Tel Aviv)	Windows; Lustre; ONTAP		✓ [1]	✓		
Oriente Médio (Barém)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Oriente Médio (Emirados Árabes Unidos)			✓ [1]	✓		
América do Sul (São Paulo)		✓	✓	✓		✓
AWS GovCloud (Oeste dos EUA)	Windows; Lustre; ONTAP		✓ [1]	✓		✓
AWS GovCloud (Leste dos EUA)	Windows; Lustre; ONTAP		✓ [1]	✓		✓

Uma verificação no Amazon FSx indica que FSx for Windows File Server, FSx for Lustre, FSx for ONTAP e FSx for OpenZFS são todos suportados nessa região por; caso contrário, as configurações suportadas serão listadas. AWS Backup

[1] Não há suporte para cópias entre regiões e entre contas.

AWS Backup: como funciona

AWS Backup é um serviço de backup totalmente gerenciado que facilita a centralização e a automatização do backup de dados em todos os serviços. AWS Com AWS Backup, você pode criar políticas de backup chamadas planos de backup. É possível usar esses planos para definir seus requisitos de backup, como a frequência com a qual fazer o backup de seus dados e por quanto tempo manter esses backups.

AWS Backup permite que você aplique planos de backup aos seus AWS recursos simplesmente marcando-os. AWS Backup em seguida, faz backup automático de seus AWS recursos de acordo com o plano de backup que você definiu.

As seções a seguir descrevem como AWS Backup funciona, seus detalhes de implementação e considerações de segurança.

Tópicos

Como AWS Backup funciona com os AWS serviços compatíveis

Alguns AWS serviços AWS Backup compatíveis oferecem seus próprios recursos de backup autônomos. Esses recursos estão disponíveis para você, independentemente de usar o AWS Backup ou não. No entanto, os backups criados por outros AWS serviços não estão disponíveis para governança central AWS Backup.

AWS Backup Para configurar o gerenciamento centralizado da proteção de dados de todos os serviços suportados, você deve optar por gerenciar esse serviço com AWS Backup, criar um backup sob demanda ou programar backups usando um plano de backup e armazenar seus backups em cofres de backup.

Tópicos

- Trabalhar com o Amazon DynamoDB
- Trabalhar com os sistemas de arquivos do Amazon FSx
- Trabalhar com o Amazon EC2
- Trabalhar com o Amazon EFS
- Trabalhar com o Amazon EBS
- Trabalhar com o Amazon RDS e o Aurora
- Trabalhando com AWS BackInt
- Trabalhando com AWS Storage Gateway
- Trabalhar com o Amazon DocumentDB
- Trabalhar com o Amazon Neptune
- Trabalhar com o Amazon Timestream
- Trabalhando com AWS Organizations
- Trabalhando com AWS CloudFormation
- Trabalhando com AWS BackInt, AWS Systems Manager para SAP e SAP HANA
- Como AWS os serviços fazem backup de seus próprios recursos

Opte por gerenciar serviços com AWS Backup

Quando novos AWS serviços estiverem disponíveis, você deverá AWS Backup habilitar o uso desses serviços. Se você tentar criar um backup sob demanda ou um plano de backup usando recursos de um serviço que não esteja habilitado, você receberá uma mensagem de erro e não poderá concluir o processo.

O AWS Backup console tem duas maneiras de incluir tipos de recursos em um plano de backup: atribuir explicitamente o tipo de recurso em um plano de backup ou incluir todos os recursos. Veja os pontos abaixo para entender como essas seleções funcionam com as inclusões no serviço.

- Se as atribuições de recursos forem baseadas somente em tags, as configurações de inclusão no serviço serão aplicadas.
- Se um tipo de recurso for explicitamente atribuído a um plano de backup, ele será incluído no backup mesmo que o opt-in não esteja habilitado para esse serviço específico. Isso não se aplica ao Aurora, ao Neptune e ao Amazon DocumentDB. Para que esses serviços sejam incluídos, o opt-in deve estar ativado.

- Se o tipo de recurso e as tags forem especificados em uma atribuição de recurso, os tipos de recursos especificados serão filtrados primeiro e, em seguida, as tags filtrarão ainda mais esses recursos.

  As configurações de aceitação do serviço são ignoradas na maioria dos tipos de recursos. No entanto, o Aurora, o Neptune e o Amazon DocumentDB exigem a aceitação do serviço.
- Para o Amazon FSx for NetApp ONTAP, ao usar a seleção de recursos com base em tags, aplique tags em volumes individuais em vez de em todo o sistema de arquivos.

As configurações de aceitação do serviço são específicas para uma região. Quando uma conta usa AWS Backup (cria um cofre de backup ou um plano de backup) em uma região, a conta é automaticamente incluída em todos os tipos de recursos suportados pela AWS Backup região naquele momento. Os serviços suportados adicionados a essa região em uma data posterior não serão incluídos automaticamente em um plano de backup. Você pode optar por optar por esses tipos de recursos assim que eles se tornarem compatíveis.

Para configurar os serviços usados com AWS Backup

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Configurações.
3. Na página Optar pela adoção do serviço, escolha Configurar recursos.
4. Use as chaves seletoras para ativar ou desativar os serviços usados com. AWS Backup

   > **Important**
   >
   > O RDS, o Aurora, o Neptune e o DocumentDB compartilham o mesmo é Nome do recurso da amazon (ARN). Optar por gerenciar um desses tipos de recursos com a AWS Backup opção de aceitar todos eles ao atribuí-lo a um plano de backup. Independentemente disso, recomendamos que você opte por todos eles para representar com precisão seu status de inscrição.
5. Selecione a opção Confirmar.

Trabalhar com dados do Amazon S3

AWS Backup oferece backup e restauração totalmente gerenciados para backups do Amazon S3. Para saber mais, consulte Backups do Amazon S3.

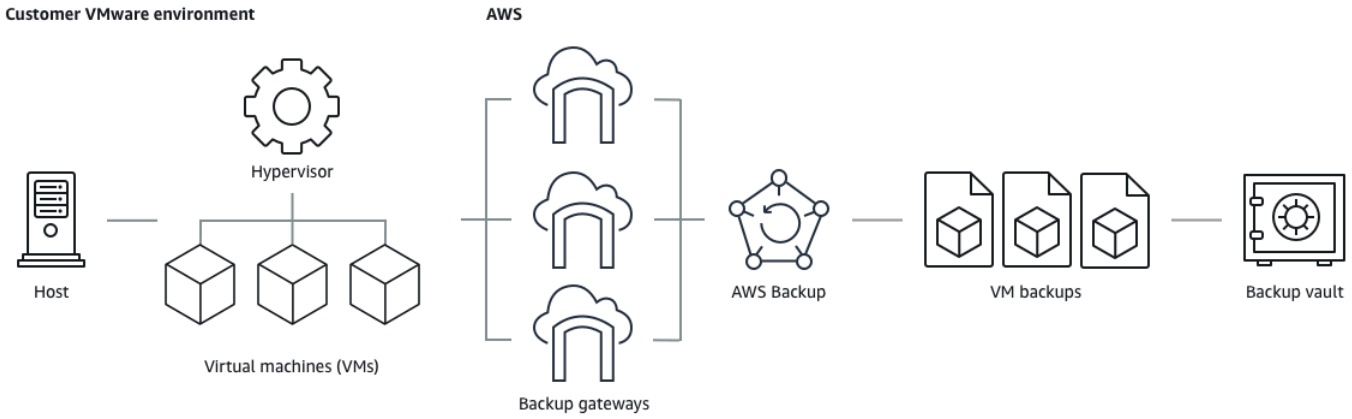
- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar dados do Amazon S3 usando: AWS BackupRestaurar dados do S3

Para obter mais informações sobre os dados do S3, consulte a documentação do Amazon S3.

Trabalhar com máquinas virtuais da VMware

AWS Backup oferece suporte à proteção de dados centralizada e automatizada para máquinas virtuais (VMs) VMware locais junto com VMs no VMware Cloud™ (VMC) ativado. AWS Você pode fazer backup de suas máquinas virtuais locais e VMC para o. AWS Backup Em seguida, você pode restaurar AWS Backup a partir do local ou do VMC.

O gateway de backup é um AWS Backup software disponível para download que você implanta em suas VMs VMware para conectá-las. AWS Backup O Backup Gateway se conecta ao seu servidor de gerenciamento de VM para descobrir VMs, descobrir suas VMs, criptografar dados e transferir dados de forma eficiente para o AWS Backup. O diagrama a seguir mostra como o Backup Gateway se conecta às suas VMs:



- Como fazer backup de recursos: Backups de máquinas virtuais
- Como restaurar os recursos da VM: Restaurando uma máquina virtual usando AWS Backup

Trabalhar com o Amazon DynamoDB

AWS Backup suporta backup e restauração de tabelas do Amazon DynamoDB. O DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que proporciona uma performance rápida e previsível, com escalabilidade contínua.

Desde seu lançamento, sempre AWS Backup apoiou o DynamoDB. A partir de novembro de 2021, AWS Backup também introduziu recursos avançados para backups do DynamoDB. Esses recursos avançados incluem copiar seus backups Regiões da AWS e contas, classificar os backups em camadas para armazenamento frio e usar tags para permissões e gerenciamento de custos.

A integração de novos AWS Backup clientes após novembro de 2021 terá os recursos avançados de backup do DynamoDB habilitados por padrão.

Recomendamos que todos os AWS Backup clientes existentes habilitem recursos avançados para o DynamoDB. Não há diferença no preço do armazenamento de backup quente depois de habilitar os recursos avançados, e você pode economizar dinheiro dividindo os backups em camadas no armazenamento frio e otimizando seus custos usando tags de alocação de custos.

Para obter uma lista completa dos recursos avançados, consulte Backup avançado do DynamoDB.

- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar os recursos do DynamoDB: Restaurar uma tabela do Amazon DynamoDB

Para obter informações detalhadas sobre o DynamoDB, consulte O que é o Amazon DynamoDB? no Guia do desenvolvedor do Amazon DynamoDB.

Trabalhar com os sistemas de arquivos do Amazon FSx

AWS Backup suporta backup e restauração de sistemas de arquivos Amazon FSx. O Amazon FSx fornece sistemas de arquivos de terceiros totalmente gerenciados com compatibilidade nativa e conjuntos de recursos para cargas de trabalho. AWS Backup usa a funcionalidade de backup integrada do Amazon FSx. Portanto, os backups feitos do console do AWS Backup têm o mesmo nível de consistência e performance do sistema de arquivos e as mesmas opções de restauração dos backups feitos pelo console do Amazon FSx.

Se você usa AWS Backup para gerenciar esses backups, obtém funcionalidades adicionais, como opções de retenção ilimitadas e a capacidade de criar backups agendados com a mesma frequência a cada hora. Além disso, AWS Backup retém seus backups mesmo após a exclusão do sistema de arquivos de origem. Isso protege contra exclusões acidentais ou mal-intencionadas.

Use AWS Backup para proteger os sistemas de arquivos Amazon FSx se quiser configurar políticas de backup e monitorar tarefas de backup a partir de um console de backup central que também estende o suporte a outros AWS serviços.

- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar recursos do Amazon FSx: Restaurar um sistema de arquivos do FSX

Para obter informações detalhadas sobre os sistemas de arquivos do Amazon FSx, consulte a documentação do Amazon FSx.

Trabalhar com o Amazon EC2

AWS Backup suporta instâncias do Amazon EC2.

- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar recursos do Amazon EC2: Restaurar uma instância do Amazon EC2

Você pode programar ou realizar trabalhos de backup sob demanda que incluam instâncias EC2 inteiras, incluindo seus volumes Amazon EBS. Portanto, você pode restaurar uma instância inteira do Amazon EC2 a partir de um único ponto de recuperação, incluindo o volume raiz, os volumes de dados e algumas definições de configuração da instância, como o tipo de instância e o par de chaves.

Também é possível fazer o backup e a restauração de aplicações do Microsoft Windows habilitadas para VSS. Você pode programar backups consistentes com aplicações, definir políticas de ciclo de vida e realizar restaurações consistentes como parte de um backup sob demanda ou de um plano de backup programado. Para ter mais informações, consulte Criar backups do VSS do Windows.

AWS Backup não reinicializa suas instâncias do EC2 em nenhum momento.

Imagens e instantâneos

Ao fazer backup de uma instância do Amazon EC2 AWS Backup , tira um instantâneo do volume de armazenamento raiz do Amazon EBS, das configurações de execução e de todos os volumes associados do EBS. AWS Backup armazena determinados parâmetros de configuração da instância do EC2, incluindo tipo de instância, grupos de segurança, Amazon VPC, configuração de monitoramento e tags. Os dados de backup são armazenados como uma imagem de máquina da Amazon (AMI) baseada em volume do Amazon EBS.

Se você excluir uma Amazon Machine Image (AMI) ou um snapshot do Amazon EBS que é gerenciado AWS Backup usando AWS Backup e tiver a lixeira do Amazon EC2 configurada, a imagem ou o snapshot poderão incorrer em cobranças de acordo com a política de lixeira do

Amazon EC2. Snapshots e imagens na lixeira do Amazon EC2 não são mais gerenciados e não serão AWS Backup gerenciados AWS Backup por políticas se você os restaurar da lixeira.

AWS Backup snapshots gerenciados do Amazon EBS e snapshots associados a uma AMI gerenciada do AWS Backup Amazon EC2 que tenham o Amazon EBS Snapshot Lock aplicado não podem ser excluídos como parte do ciclo de vida do ponto de recuperação se a duração do bloqueio do snapshot exceder o ciclo de vida do backup. Em vez disso, esses pontos de recuperação terão um status de `EXPIRED`. Esses pontos de recuperação poderão ser excluídos manualmente se você optar por começar removendo o Bloqueio de Snapshots do Amazon EBS.

AWS Backup pode criptografar snapshots do EBS associados a um backup do Amazon EC2. Isso é semelhante à forma como ele criptografa os snapshots do EBS. AWS Backup usa a mesma criptografia aplicada aos volumes subjacentes do EBS ao criar um snapshot da AMI do Amazon EC2, e os parâmetros de configuração da instância original persistem nos metadados de restauração.

Um instantâneo deriva sua criptografia do volume, e a mesma criptografia é aplicada aos instantâneos correspondentes. Os snapshots do EBS de uma AMI copiada são sempre criptografados. Se você especificar uma chave KMS durante a cópia, a chave especificada será aplicada. Se você não especificar uma chave KMS, uma chave KMS padrão será aplicada.

Para obter mais informações, consulte as instâncias do Amazon EC2 no Guia do usuário do Amazon EC2 e a criptografia do Amazon EBS no Guia do usuário do Amazon EBS.

Trabalhar com o Amazon EFS

AWS Backup é compatível com o Amazon Elastic File System (Amazon EFS).

- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar recursos do Amazon EFS: Restaurar um sistema de arquivos do Amazon EFS

Para obter informações detalhadas sobre os sistemas de arquivos do Amazon EFS, consulte O que é o Amazon Elastic File System? no Guia do usuário do Amazon Elastic File System.

Trabalhar com o Amazon EBS

AWS Backup oferece suporte aos volumes do Amazon Elastic Block Store (Amazon EBS).

AWS Backup snapshots gerenciados do Amazon EBS e snapshots associados a uma AMI gerenciada do AWS Backup Amazon EC2 que tenham o Amazon EBS Snapshot Lock aplicado não podem ser excluídos como parte do ciclo de vida do ponto de recuperação se a duração do bloqueio

do snapshot exceder o ciclo de vida do backup. Em vez disso, esses pontos de recuperação terão um status de `EXPIRED`. Esses pontos de recuperação poderão ser excluídos manualmente se você optar por começar removendo o Bloqueio de Snapshots do Amazon EBS.

- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar volumes do Amazon EBS: Restaurar um volume do Amazon EBS

Para obter mais informações, consulte os volumes do Amazon EBS no Guia do usuário do Amazon EBS.

Trabalhar com o Amazon RDS e o Aurora

AWS Backup oferece suporte aos mecanismos de banco de dados do Amazon RDS e aos clusters Aurora.

- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar recursos do Amazon RDS: Restaurar um banco de dados do RDS
- Como restaurar clusters do Aurora: Restaurar um cluster do Aurora

Para obter mais informações sobre o Amazon RDS, consulte O que é o Amazon Relational Database Service? no Guia do usuário do Amazon RDS.

Para obter informações detalhadas sobre o Aurora, consulte O que é o Amazon Aurora? no Guia do usuário do Amazon Aurora.

> **Note**
>
> Se você iniciar um trabalho de backup no console do Amazon RDS, isso pode entrar em conflito com um trabalho de backup de clusters do Aurora, fazendo com que o erro O trabalho de backup expirou antes da conclusão seja exibido. Se isso ocorrer, configure uma janela de backup mais longa no AWS Backup.

> **Note**
>
> O RDS Custom for SQL Server e o RDS Custom for Oracle não são compatíveis com o AWS Backup no momento.

> **Note**
>
> AWS não cobra pelos instantâneos do Aurora armazenados em um cofre de backup, desde que o Aurora tenha os backups automatizados habilitados e o período de retenção dos backups automatizados do Aurora seja maior do que o período de retenção dos instantâneos do Aurora. Todos os snapshots no cofre de backup serão cobrados se o banco de dados dos snapshots for excluído (as exclusões podem ocorrer acidentalmente ou durante a implantação azul/verde).
> Snapshots grandes e backups frequentes de um banco de dados excluído podem resultar em custos significativos de armazenamento. Acesse a Calculadora do AWS Backup para estimar possíveis cobranças do AWS Backup .

Trabalhando com AWS BackInt

AWS Backup trabalha com o AWS Backint para oferecer suporte ao backup e restauração do banco de dados SAP HANA nas instâncias do Amazon EC2.

- Instruções para fazer backup e restaurar recursos do SAP HANA: backup e restauração de instâncias do SAP HANA Amazon EC2
- Configurar o AWS Backint Agent AWS : Backint Agent para SAP HANA

Trabalhando com AWS Storage Gateway

AWS Backup suporta o Storage Gateway Volume Gateway. Você também pode restaurar snapshots do Amazon EBS como volumes do Storage Gateway.

- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar recursos do Storage Gateway: Restaurar um volume do Storage Gateway.

Trabalhar com o Amazon DocumentDB

AWS Backup é compatível com clusters Amazon DocumentDB.

- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar os recursos do Amazon DocumentDB:. Restaurar um cluster do DocumentDB

Trabalhar com o Amazon Neptune

AWS Backup oferece suporte aos clusters do Amazon Neptune.

- Como fazer backup de recursos: Começando com AWS Backup
- Como restaurar clusters do Amazon Neptune: Restaurar um cluster do Neptune.

Trabalhar com o Amazon Timestream

AWS Backup suporta tabelas Amazon Timestream.

- Como fazer backup de tabelas do Timestream.
- Como restaurar tabelas do Timestream.

Trabalhando com AWS Organizations

AWS Backup trabalha com AWS Organizations para simplificar o monitoramento e o gerenciamento de várias contas

- Crie uma conta de gerenciamento no Organizations.
- Ative o gerenciamento entre contas.
- Designe as contas de administrador delegado e políticas delegadas.

Trabalhando com AWS CloudFormation

AWS Backup AWS CloudFormation modelos de suporte e pilhas de aplicativos

- AWS CloudFormation backups em pilha

Trabalhando com AWS BackInt, AWS Systems Manager para SAP e SAP HANA

AWS Backup trabalha com AWS BackInt e com o SSM for SAP para oferecer suporte às funções de backup e restauração do SAP HANA.

- Backup de bancos de dados SAP HANA em instâncias do Amazon EC2

- Comece a usar AWS Systems Manager para SAP
- AWS Backint Agent para SAP HANA

Como AWS os serviços fazem backup de seus próprios recursos

Você pode consultar a documentação técnica do processo de backup e restauração de um AWS serviço específico, especialmente quando, durante uma restauração, você precisa configurar uma nova instância desse AWS serviço. Veja a seguir uma lista da documentação:

- Serviços relacionados ao Amazon EC2
- Usando AWS Backup com o Amazon EFS
- Backup e restauração sob demanda para o DynamoDB
- Snapshots do Amazon EBS
- Backup e restauração de instâncias de banco de dados do Amazon RDS
  - Visão geral do backup e da restauração de um cluster de banco de dados do Aurora
- Usando AWS Backup com FSx for Windows File Server
- Usando AWS Backup com FSx for Lustre
- Fazendo backup de seus volumes em AWS Storage Gateway
- Backup e restauração no Amazon DocumentDB
- Backup e a restauração de um cluster de banco de dados do Amazon Neptune

Medição, custos e cobrança

AWS Backup preços

AWS Backup Os preços atuais estão disponíveis em AWS Backup pricing.

> **Important**
>
> Para evitar cobranças adicionais, configure sua política de retenção com uma duração de armazenamento quente de pelo menos uma semana.
> Por exemplo, suponha que você faça backups diários e os retenha por um dia. Além disso, suponha que seus recursos protegidos sejam tão grandes que seja necessário um dia inteiro para concluir o backup. AWS Backup implementa o período de retenção de um dia

e remove o backup do armazenamento aquecido quando a tarefa de backup é concluída. No dia seguinte, AWS Backup não é possível criar um backup incremental porque você não tem backup em armazenamento aquecido. Como esse período de retenção não seguiu as práticas recomendadas, você corre o risco e a despesa de criar um backup completo todos os dias.
Entre em contato AWS Support para obter mais assistência.

AWS Backup faturamento

Quando um tipo de recurso oferece suporte ao AWS Backup gerenciamento total, as cobranças pela AWS Backup atividade (incluindo armazenamento, transferências de dados, restaurações e exclusão antecipada) aparecem na seção “Backup” da sua Amazon Web Services fatura. Para obter uma lista dos serviços que oferecem suporte ao AWS Backup gerenciamento completo, consulte a seção AWS Backup Gerenciamento completo na Disponibilidade de recursos por recurso tabela.

Quando um tipo de recurso não oferece suporte ao AWS Backup gerenciamento total, algumas de suas AWS Backup atividades, como os custos de armazenamento de seus backups, têm a cobrança refletida pelo respectivo AWS serviço.

Falhas na tarefa de cópia

Você só será cobrado quando um ponto de recuperação for criado no cofre de destino. Não há cobrança quando há falha em um trabalho de cópia e nenhum ponto de recuperação é criado.

Tags de alocação de custos

Você pode usar tags de alocação de custos para rastrear e otimizar AWS Backup custos em um nível detalhado e visualizar e filtrar essas tags usando AWS Cost Explorer.

Para usar tags de alocação de custos, consulte Automatizar backups e otimizar custos de backup para o Amazon EFS usando o AWS Backup e Usar tags de alocação de custos.

AWS Backup Preços do Audit Manager

AWS Backup O Audit Manager cobra pelo uso com base no número de avaliações de controle. Uma avaliação de controle é a avaliação de um recurso em relação a um controle. As cobranças de avaliação de controle aparecem em sua AWS Backup fatura. Para ver a definição de preço atual das avaliações de controle, consulte Definição de preço do AWS Backup.

Para usar os controles do AWS Backup Audit Manager, você deve habilitar a AWS Config gravação para rastrear sua atividade de backup. AWS Config cobranças para cada item de configuração registrado, e essas cobranças aparecem na sua AWS Config fatura. Para ver a definição de preço registrado do item de configuração atual, consulte Definição de preço do AWS Config.

Definição de preço do Amazon Aurora

Durante o período de retenção configurado para backups contínuos do Aurora (até 35 dias), os snapshots não incorrem em cobrança de armazenamento. Os snapshots retidos após essa janela serão cobrados como backups completos.

AWS Backup blogs, vídeos, tutoriais e outros recursos

Para obter mais informações sobre AWS Backup, consulte o seguinte:

- Faça backup e restaure máquinas virtuais VMware locais usando. AWS Backup Com Olumuyiwa Koya e Ezekiel Oyerinde (junho de 2022).
- Usando AWS Backup para proteger bancos de dados Amazon Aurora. Com Chris Hendon, Brandon Rubadou e Thomas Liddle (maio de 2022).
- Proteja instâncias criptografadas do Amazon RDS com backups entre contas e regiões. Com Evan Peck e Sabith Venkitachalapathy (maio de 2022).
- Automatize e melhore sua postura de segurança usando e. AWS BackupAWS PrivateLink Com Bilal Alam (abril de 2022).
- Obtenha relatórios AWS Backup multirregionais agregados diários entre contas. Com Wali Akbari e Sabith Venkitachalapathy (fevereiro de 2022).
- Automatize a visibilidade das descobertas de backup usando AWS Backup e. AWS Security Hub Com Kanishk Mahajan (janeiro de 2022).
- As 10 melhores práticas de segurança para proteger backups em AWS. Com Ibukun Oyewumi (janeiro de 2022).
- Otimizando o SAS Grid AWS com o FSx for Lustre (e otimizando a recuperação de desastres usando). AWS Backup Com Matt Saeger e Shea Lutton (janeiro de 2022).
- Centralizando a proteção e a conformidade de dados no Amazon Neptune com. AWS Backup Com Brian O'Keefe (novembro de 2021).
- Gerencie o backup e a restauração do Amazon DocumentDB (compatível com MongoDB) com o AWS Backup. Com Karthik Vijayraghavan (novembro de 2021).

- Simplifique a auditoria de suas políticas de proteção de dados com o AWS Backup Audit Manager. Com Jordan Bjorkman e Harshitha Putta (novembro de 2021).
- Melhore a postura de segurança de seus backups com o AWS Backup Vault Lock. Com Rolland Miller (outubro de 2021).
- Como reter etiquetas de recursos em trabalhos de AWS Backup restauração. Com Ibukun Oyewumi, Amee Shah e Sabith Venkitachalapathy (setembro de 2021).
- Gerenciando o acesso aos backups usando políticas de controle de serviços com AWS Backup. Com Sabith Venkitachalapathy e Ibukun Oyewumi (agosto de 2021).
- Automatize o backup centralizado em escala em todos os AWS serviços usando. AWS Backup Com Ibukun Oyewumi e Sabith Venkitachalapathy (julho de 2021).
- Blog: Como simplificar o backup do Microsoft SQL Server usando AWS Backup um VSS. Com Siavash Irani e Sepehr Samiei (julho de 2021).
- Automatize a validação da recuperação de dados com AWS Backup. Com Mahanth Jayadeva (junho de 2021).
- Configurando notificações para monitorar AWS Backup trabalhos. Com Virgil Ennes (junho de 2021).
- Automatize backups e otimize os custos de backup para o Amazon EFS usando o AWS Backup. Com Prachi Gupta e Rohit Verma (junho de 2021).
- Gerencie os custos de backup do Amazon EFS: AWS Backup suporte para tags de alocação de custos. Com Aditya Maruvada (maio de 2021).
- Crie e compartilhe backups criptografados entre contas e regiões usando AWS Backup. Com Prachi Gupta (maio de 2021).
- AWS Backup agora é aprovado pelo FedRAMP High para suas necessidades de conformidade e proteção de dados. Com Andy Grimes (maio de 2021).
- A ZS Associates aprimora a eficiência do backup com. AWS Backup Com Mitesh Naik, Hiranand Mulchandani e Sushant Jadhav (maio de 2021).
- Tutorial: Backup e restauração do Amazon EBS usando AWS Backup. Com Fathima Kamal (abril de 2021).
- Tutorial em vídeo: Gerencie cópias de backups entre regiões. Com David DeLuca (abril de 2021).
- Exclua vários pontos AWS Backup de recuperação usando o AWS Tools for PowerShell. Com Sherif Talaat (abril de 2021).
- Backups entre regiões e entre contas para uso do Amazon FSx. AWS Backup Com Adam Hunter e Fathima Kamal (abril de 2021).

- CloudWatch Eventos e métricas da Amazon para AWS Backup. Com Rolland Miller (março de 2021).
- Tutorial: Backup e restauração do Amazon Relational Database Service (RDS) usando. AWS Backup Com Fathima Kamal (março de 2021).
- oint-in-time Recuperação P e backup contínuo para Amazon RDS com AWS Backup. Com Kelly Griffin (março de 2021).
- Automatize AWS Backup com AWS Service Catalog. com John Husemoller (janeiro de 2021).
- Recuperação segura de dados com backup entre contas e cópias entre regiões usando o AWS Backup. Com Cher Simon (janeiro de 2021).
- AWS Resumo do re:Invent: Proteção de dados e conformidade com. AWS Backup Com Nancy Wang (dezembro de 2020).
- AWS Backup fornece proteção de dados centralizada em todos os seus AWS recursos. Com Nancy Wang (novembro de 2020).
- Tech Talk: Proteção de dados em grande escala com o AWS Backup. Com Kareem Behairy (setembro de 2020).
- Gerenciamento centralizado de várias contas com uso de cópias entre regiões. AWS Backup Com Cher Simon (setembro de 2020).
- Tutorial em vídeo: Gerenciando backups em grande escala em seu AWS Organizations uso AWS Backup. Com Ildar Sharafeev (julho de 2020).
- Gerenciando backups em grande escala em seu AWS Organizations uso AWS Backup. Com Nancy Wang, Avi Drabkin, Ganesh Sundaresan e Vikas Shah (junho de 2020).
- Recupere arquivos e pastas do Amazon EFS com AWS Backup o. Com Abrar Hussain e Gurudath Pai (maio de 2020).
- Programar backups automatizados usando o Amazon EFS e o AWS Backup. Com Rob Barnes (dezembro de 2019).
- Gravação re:Invent: AWS re:Invent 2019: mergulho profundo em pés AWS Backup Rackspace. Com Nancy Wang e Jason Pavao (dezembro de 2019).
- Protegendo seus dados com AWS Backup. Com Anthony Fiore (julho de 2019).
- Vídeo de marketing: Apresentação do AWS Backup. Janeiro de 2019.
- Vídeo: Introdução ao AWS Backup. Com AWS treinamento e certificação.

Configurando AWS pela primeira vez

Antes de usar AWS Backup pela primeira vez, conclua as seguintes tarefas:

1. Inscreva-se para AWS
2. Criar um usuário do IAM
3. Criar um perfil do IAM

Inscreva-se para AWS

Quando você se inscreve no Amazon Web Services (AWS), você Conta da AWS se inscreve automaticamente em todos os serviços em AWS, inclusive AWS Backup. Você será cobrado apenas pelos serviços que usar.

Para obter mais informações sobre taxas de AWS Backup uso, consulte a página AWS Backup de preços.

Se você Conta da AWS já tiver um, vá para a próxima tarefa. Se você ainda não possuir uma conta da AWS , use o procedimento a seguir para criar uma.

Para criar um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

Anote seu Conta da AWS número, pois você precisará dele para a próxima tarefa.

Criar um usuário do IAM

Serviços em AWS, como AWS Backup, exigem que você forneça credenciais ao acessá-los, para que o serviço possa determinar se você tem permissões para acessar seus recursos. AWS recomenda que você não use o usuário Conta da AWS root para fazer solicitações. Em vez disso, crie um usuário do IAM e conceda acesso total a esse usuário. Esses usuários são conhecidos como usuários administradores. Você pode usar as credenciais do usuário administrador, em vez das credenciais do usuário Conta da AWS raiz, para interagir AWS e realizar tarefas, como criar um bucket, criar usuários e conceder permissões a eles. Para obter mais informações, consulte Credenciais de usuário raiz da Conta da AWS vs. credenciais de usuário do IAM na Referência geral da AWS e Práticas recomendadas do IAM no Guia do usuário do IAM.

Se você se inscreveu AWS , mas não criou um usuário do IAM para si mesmo, você pode criar um usando o console do IAM.

Para criar um usuário administrador, selecione uma das opções a seguir.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
Centro de Identidade do IAM (Recomendado)	Use credenciais de curto prazo para acessar a AWS. Isso está de acordo com as práticas recomendadas de segurança. Para obter informações sobre as práticas recomendadas, consulte Práticas recomendadas de	Seguindo as instruções em Conceitos básicos no Guia do usuário do AWS IAM Identity Center .	Configure o acesso programático configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
	segurança no IAM no Guia do usuário do IAM.		
No IAM (Não recomendado)	Use credenciais de curto prazo para acessar a AWS.	Seguindo as instruções em Criar o seu primeiro usuário administrador e um grupo de usuários do IAM no Guia do usuário do IAM.	Para configurar o acesso programático, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM.

Para entrar como esse novo usuário do IAM, saia do AWS Management Console. Em seguida, use o seguinte URL, em que your_aws_account_id é seu Conta da AWS número sem os hífens (por exemplo, se seu número for, seu ID será): Conta da AWS `1234-5678-9012` Conta da AWS `123456789012`

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

Insira o nome e a senha de usuário do IAM que você acabou de criar. Após fazer login, a barra de navegação exibirá your_user_name@your_aws_account_id.

Se você não quiser que o URL da sua página de login contenha seu Conta da AWS ID, você pode criar um alias de conta. No painel do IAM;, clique em Criar alias da conta e insira um alias. Por exemplo, o nome de sua empresa. Para fazer o login depois de criar o alias de uma conta, use o seguinte URL:

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

Para verificar o link de login para usuários do IAM de sua conta, abra o console do IAM e confira em Alias da Conta da AWS no painel.

Criar um perfil do IAM

Você pode usar o console do IAM para criar uma função do IAM que conceda AWS Backup permissões para acessar recursos compatíveis. Depois de criar o perfil do IAM, você poderá criar e associar políticas ao perfil.

Como criar uma perfil do IAM com o console

1. Faça login no AWS Management Console e abra o console do IAM.
2. No console do IAM, escolha Perfis no painel de navegação, e escolha Criar perfil.
3. Escolha Perfis de serviço do AWS e, em seguida, escolha Selecionar para AWS Backup. Escolha Próximo: permissões.
4. Na página Anexar políticas de permissões, marque `AWSBackupServiceRolePolicyForBackup` e `AWSBackupServiceRolePolicyForRestores`. Essas políticas AWS gerenciadas concedem AWS Backup permissão para fazer backup e restaurar todos os AWS recursos compatíveis. Para saber mais sobre as políticas gerenciadas e ver exemplos, consulte Políticas gerenciadas.

   Em seguida, escolha Próximo: Tags.
5. Escolha Próximo: revisar.
6. Em Nome da função, digite um nome que descreva a finalidade da função. Os nomes das funções devem ser exclusivos em seu Conta da AWS. Como várias entidades podem fazer referência à função, não é possível editar o nome da função depois de sua criação.

   Selecione Criar função.
7. Na página Funções, escolha a função que você criou, para abrir a página de detalhes.

Começando com AWS Backup

Este tutorial mostra as etapas genéricas para usar AWS Backup recursos e funcionalidades. Como em qualquer parte desta documentação técnica, você deve acompanhar o AWS Management Console na outra janela.

Você também pode aprender a usar AWS Backup com um serviço específico lendo estes tutoriais:

- Backup e restauração do Amazon Relational Database Service (Amazon RDS) usando AWS Backup
- Tutorial: Backup e restauração do Amazon EBS usando AWS Backup

Tópicos

Pré-requisitos

Antes de começar, verifique se você tem:

- Um Conta da AWS. Para ter mais informações, consulte Configurando AWS pela primeira vez.
- Pelo menos um recurso suportado pelo AWS Backup.
- Você deve estar familiarizado com os AWS serviços e recursos dos quais está fazendo backup. Veja a lista de Recursos da AWS compatíveis e aplicações de terceiros.

  Quando novos AWS serviços estiverem disponíveis, habilite AWS Backup o uso desses serviços.

Para configurar os AWS serviços a serem usados com AWS Backup

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Configurações.
3. Na página Optar pela adoção do serviço, escolha Configurar recursos.
4. Na página Configurar recursos, use as opções de alternância para ativar ou desativar os serviços usados com. AWS Backup Escolha Confirmar quando os serviços estiverem configurados. Certifique-se de que o AWS serviço que você está optando esteja disponível no seu Região da AWS.

Consulte Atribuir recursos a um plano de backup para obter informações adicionais. O AWS Backup console permite que um usuário atribua um tipo de recurso a um plano de backup; isso será incluído mesmo que o opt-in não esteja habilitado para esse serviço específico.

- Certifique-se de que os recursos dos quais você está fazendo backup estejam todos na mesma Região da AWS.

Para concluir este tutorial, você pode usar seu usuário Conta da AWS root para fazer login no AWS Management Console. No entanto, o AWS Identity and Access Management (IAM) recomenda que você não use o usuário Conta da AWS root. Em vez disso, crie um perfil de administrador em sua conta e use essas credenciais para gerenciar os recursos dela. Para ter mais informações, consulte Configurando AWS pela primeira vez.

O AWS Backup console oferece opções diferentes para fazer backup de seus recursos. Você pode criar um backup sob demanda, programar e configurar como deseja que o backup do recurso seja feito ou configurar recursos para backup automático quando o recurso for criado.

Conceitos básicos 1: inclusão no serviço

O AWS Backup console tem duas maneiras de incluir tipos de recursos em um plano de backup: atribuir explicitamente o tipo de recurso em um plano de backup ou incluir todos os recursos. Veja os pontos abaixo para entender como essas seleções funcionam com as inclusões no serviço.

- Se as atribuições de recursos forem baseadas somente em tags, as configurações de inclusão no serviço serão aplicadas.

- Se um tipo de recurso for explicitamente atribuído a um plano de backup, ele será incluído no backup mesmo que o opt-in não esteja habilitado para esse serviço específico. Isso não se aplica ao Aurora, ao Neptune e ao Amazon DocumentDB. Para que esses serviços sejam incluídos, o opt-in deve estar ativado.
- Se o tipo de recurso e as tags forem especificados em uma atribuição de recurso, os tipos de recursos especificados serão filtrados primeiro e, em seguida, as tags filtrarão ainda mais esses recursos.

  As configurações de aceitação do serviço são ignoradas na maioria dos tipos de recursos. No entanto, o Aurora, o Neptune e o Amazon DocumentDB exigem a aceitação do serviço.
- Para o Amazon FSx for NetApp ONTAP, ao usar a seleção de recursos com base em tags, aplique tags em volumes individuais em vez de em todo o sistema de arquivos.

As opções de aceitação se aplicam à conta específica e. Região da AWS Quando uma conta usa AWS Backup (cria um cofre de backup ou um plano de backup) em uma região, a conta é automaticamente incluída em todos os tipos de recursos suportados pela AWS Backup região naquele momento. Os serviços suportados adicionados a essa região em uma data posterior não serão incluídos automaticamente em um plano de backup. Você pode optar por optar por esses tipos de recursos assim que eles se tornarem compatíveis.

Como AWS Backup oferece suporte a cada vez mais AWS serviços e aplicativos de terceiros, talvez seja necessário revisar esta etapa para optar por esses recursos recém-suportados.

AWS Backup não controla nem gerencia backups feitos em outros AWS ambientes que AWS Backup não sejam.

Para optar por usar AWS Backup para proteger todos os tipos de recursos suportados

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação à esquerda, escolha Configurações.
3. Em Inclusão do serviço, escolha Configurar recursos.
4. Opte por todos os recursos AWS Backup suportados movendo todos os botões para a direita.
5. Selecione Confirmar.

Próximas etapas

Para criar um backup sob demanda usando AWS Backup, prossiga paraConceitos básicos 2: criar um backup sob demanda.

Conceitos básicos 2: criar um backup sob demanda

No AWS Backup console, a página Recursos protegidos lista os recursos que foram copiados pelo AWS Backup menos uma vez. Se você estiver usando AWS Backup pela primeira vez, não há recursos, como volumes do Amazon EBS ou bancos de dados do Amazon RDS, listados nesta página. Isso se aplica mesmo se esse recurso foi atribuído a um plano de backup, caso esse plano de backup não tenha executado uma tarefa de backup programada pelo menos uma vez.

Nesta etapa, você criará um backup sob demanda de um dos seus recursos. Você verá esse recurso listado na página Recursos protegidos.

Como criar um backup sob demanda

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Ou, usando o painel de navegação, escolha Recursos protegidos e Criar backup sob demanda.
3. Na página Criar backup sob demanda, escolha o tipo de recurso do qual você deseja fazer backup. Por exemplo, escolha DynamoDB para tabelas do Amazon DynamoDB.
4. Escolha o nome e o ID do recurso que você deseja proteger. Certifique-se de que o recurso escolhido seja o que você deseja.

   > **Note**
   >
   > Para o Amazon FSx para Lustre, os tipos de implantação Persistent e Persistent_2 são compatíveis.

5. Certifique-se de que a opção Criar backup agora esteja selecionada. Isso inicia um backup imediatamente e permite que você consulte antes o recurso salvo na página Recursos protegidos.
6. Especifique uma transição para valor de armazenamento frio (se necessário) e um valor de expiração.

> **Note**
>
> - Para ver a lista de recursos que podem fazer a transição para o armazenamento frio, consulte a seção “Ciclo de vida para o armazenamento frio da tabela Disponibilidade de recursos por recurso. Todos os outros tipos de recursos são salvos em armazenamento quente e ignoram a expressão de transição para armazenamento frio. O valor de expiração é válido para todos os tipos de recursos.
> - Quando os backups expiram e são marcados para exclusão como parte de sua política de ciclo de vida, AWS Backup exclui os backups em um ponto escolhido aleatoriamente nas 8 horas seguintes. Essa janela ajuda a garantir um desempenho consistente.

7. Escolha um cofre de backup existente. Ao escolher Criar novo cofre de backup uma nova página será aberta para criar um cofre e você será redirecionado para a página Criar backup sob demanda ao concluir.
8. Em Perfil do IAM, escolha Função padrão.

> **Note**
>
> Se a função AWS Backup padrão não estiver presente na sua conta, uma função será criada para você com as permissões corretas.

9. Se você deseja atribuir uma ou mais tags ao seu backup sob demanda, insira uma chave e um valor opcional, e escolha Adicionar tag.

> **Note**
>
> - Para recursos do Amazon EC2, copia AWS Backup automaticamente as tags existentes de grupos e recursos individuais, além de todas as tags que você adicionar a esse backup. Para obter mais informações, consulte Copiar tags em objetos.
> - Ao criar um plano de backup baseado em tags, se você escolher uma função diferente da função Padrão, verifique se ela tem as permissões necessárias para fazer backup de todos os recursos marcados. AWS Backup tenta processar todos os recursos com as tags selecionadas. Se o plano de backup encontrar um recurso para o qual não tenha permissão para acessar, ele falhará.

10. Escolha Criar backup sob demanda. Dessa forma, você será redirecionado para a página Trabalhos, onde verá uma lista de trabalhos.
11. Se o seu tipo de recurso for EC2, a seção Configurações avançadas de backup será exibida. Escolha VSS do Windows se a sua instância do EC2 estiver executando o Microsoft Windows. Isso permite que você faça backups do VSS do Windows consistentes com aplicativos.

> **Note**
>
> AWS Backup atualmente oferece suporte a backups consistentes com aplicativos de recursos executados somente no Amazon EC2. Não há compatibilidade com todos os tipos de instância ou de aplicações para backups do VSS do Windows. Para ter mais informações, consulte Criar backups do VSS do Windows.

12. Escolha o ID do trabalho de backup do recurso para o qual você optou por fazer backup para ver os detalhes desse trabalho.

Próximas etapas

Para automatizar a atividade de backup, acesse Conceitos básicos 3: criar um backup programado.

Conceitos básicos 3: criar um backup programado

Nesta etapa do AWS Backup tutorial, você cria um plano de backup, atribui recursos a ele e, em seguida, cria um cofre de backup.

Antes de começar, verifique se você tem os pré-requisitos necessários. Para ter mais informações, consulte Começando com AWS Backup.

Tópicos

Etapa 1: criar um plano backup de com base em um existente

Um plano de backup é uma expressão de política que define quando e como você deseja fazer backup de seus recursos da AWS , como tabelas do Amazon DynamoDB ou sistemas de arquivos do Amazon Elastic File System (Amazon EFS). Você atribui recursos aos planos de backup e, AWS Backup em seguida, faz backup e retém automaticamente os backups desses recursos de acordo com o plano de backup. Para ter mais informações, consulte Gerenciar backups usando planos de backup.

Há duas maneiras de criar um novo plano de backup: você pode criar um de zero ou com base em um plano de backup existente. Este exemplo usa o AWS Backup console para criar um plano de backup modificando um plano de backup existente.

Como criar um plano de backup de um plano existente

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel, escolha Gerenciar planos de backup. Ou, usando o painel de navegação, escolha Planos de backup e Criar plano de backup.
3. Escolha Começar com um modelo, escolha um plano na lista (por exemplo, `Daily-Monthly-1yr-Retention`) e insira um nome na caixa Nome do plano de backup.

   > **Note**
   >
   > Se tentar criar um plano de backup idêntico a um plano existente, você receberá um erro `AlreadyExistsException`.

4. Na página de resumo do plano, escolha a regra de backup e escolha Editar.
5. Analise e escolha os valores que você deseja aplicar à regra (consulte Opções de planos e configuração de backup para conferir as opções para regras).
6. Para o cofre de backup, escolha Padrão ou escolha Criar cofre de backup para criar um cofre.
7. (Opcional) - escolha um na Região da AWS lista na região de destino para copiar o backup para uma região diferente. Para adicionar mais regiões, escolha Adicionar cópia.
8. Depois de concluir a edição da regra, selecione Salvar regra de backup.

Na página Resumo, escolha Atribuir recursos para se preparar para a próxima seção.

Etapa 2: atribuir recursos a um plano de backup

Depois de criar um plano de backup, você deve atribuir seus AWS recursos a esse plano de backup. Para obter mais informações sobre a atribuição de recursos, consulte Atribuir recursos a um plano de backup.

Se você ainda não tiver AWS recursos existentes que queira atribuir a um plano de backup, crie alguns novos recursos para usar neste exercício. Crie um ou dois recursos usando recursos da AWS compatíveis e aplicações de terceiros.

Como atribuir recursos a um plano de backup

1. As etapas anteriores devem ter levado você à página Atribuir recursos.
2. Digite o nome de uma atribuição de recurso.
3. Para um perfil do IAM, escolha Perfil padrão. Se você escolher outro perfil, ele deverá ter permissões para fazer backup de todos os recursos que você atribuir.
4. Na seção Atribuir recursos, escolha Incluir todos os tipos de recursos. Um tipo de recurso é um AWS serviço AWS Backup compatível ou um aplicativo de terceiros. Esse plano de backup agora protegerá todos os tipos de recursos que você optou por proteger usando AWS Backup
5. Escolha Atribuir recursos.

Você retornará à página Resumo do plano de backup. Escolha Criar plano de backup para implantar seu primeiro plano de backup.

Etapa 3: criar um cofre de backup

Em vez de usar o cofre de backup padrão que é criado automaticamente para você no console do AWS Backup , crie cofres de backup específicos para salvar e organizar grupos de backups no mesmo cofre.

Para obter mais informações sobre cofres de backups, consulte Cofres de backup.

Como criar um cofre de backup

1. No AWS Backup console, no painel de navegação, escolha Backup vaults.

> **Note**
>
> Se o painel de navegação não estiver visível no lado esquerdo, você poderá abri-lo escolhendo o ícone do menu no canto superior esquerdo do console. AWS Backup

2. Escolha Criar cofre de backup.
3. Insira um nome para o cofre de backup. Você pode nomear o cofre para refletir o que será armazenado nele ou para facilitar a pesquisa de backups necessários. Por exemplo, você pode nomeá-lo como: **`FinancialBackups`**.
4. Selecione uma tecla AWS Key Management Service (AWS KMS). Você pode usar uma chave que você já criou ou selecionar a chave AWS Backup KMS padrão.

> **Note**
>
> A AWS KMS chave especificada aqui se aplica somente aos backups de serviços que oferecem suporte à criptografia AWS Backup independente. Para ver a lista de tipos de recursos que oferecem suporte à criptografia AWS Backup independente, consulte a seção “ AWS Backup Gerenciamento completo” da Disponibilidade de recursos por recurso tabela.

5. Opcionalmente, adicione tags que ajudarão você a procurar e identificar o cofre de backup. Por exemplo, você pode adicionar uma tag **`BackupType:Financial`**.
6. Escolha Criar cofre de backup.
7. No painel de navegação, escolha Cofres de backup e verifique se o cofre de backup foi adicionado.

> **Note**
>
> Agora é possível editar uma regra de backup em um de seus planos de backup para armazenar backups criados por essa regra no cofre de backup que você acabou de criar.

Próximas etapas

Para fazer backup específico dos sistemas de arquivos do Amazon EFS, prossiga para Conceitos básicos 4: criar backups automáticos do Amazon EFS.

Conceitos básicos 4: criar backups automáticos do Amazon EFS

Ao criar um sistema de arquivos do Amazon Elastic File System (Amazon EFS) usando o console do Amazon EFS, os backups automáticos serão ativados por padrão. Se você quiser fazer backup automático de um sistema de arquivos existente do Amazon EFS, você poderá fazer isso usando o console, a API ou a CLI do Amazon EFS.

Como fazer backup automático de um sistema de arquivos existente do Amazon EFS usando o console

1. Abra o console do Amazon EFS em https://console.aws.amazon.com/efs.
2. Na página Sistemas de arquivos, escolha um sistema de arquivos para ativar os backups automáticos.
3. Escolha Editar no painel de configurações Geral.
4. Para ativar os backups automáticos, escolha Habilitar backups automáticos.

A configuração padrão do plano de backup é `daily backups, 35-day retention`. A janela de backup padrão (o período quando o backup será executado) é definida para iniciar às 5h UTC (Tempo Universal Coordenado) e dura 8 horas.

> **Note**
>
> O cofre de backup automático `aws/efs/automatic-backup-vault` do Amazon EFS é reservado somente para esses backups automáticos.
> Esse cofre não deve ser usado para criar cópias entre contas ou como destino para backups criados por outros planos de backup não automatizados. Se usá-lo como destino para outros planos de backup, você receberá um erro de “privilégios insuficientes”.

AWS Backup cria uma função vinculada ao serviço em seu nome na sua conta. Essa função tem as permissões necessárias para executar backups do Amazon EFS. Para obter informações detalhadas sobre funções vinculadas ao serviço, consulte Usar perfis vinculados a serviço do AWS Backup.

Para step-by-step obter instruções sobre como ativar ou desativar backups automáticos usando o console, a API ou a CLI do Amazon EFS, consulte Backups automáticos no Guia do usuário do Amazon Elastic File System.

Próximas etapas

Para ver os backups que você criou, prossiga para Conceitos básicos 5: visualizar suas tarefas de backup e pontos de recuperação.

Conceitos básicos 5: visualizar suas tarefas de backup e pontos de recuperação

Com AWS Backup, você pode visualizar o status e outros detalhes da atividade de backup e restauração nos AWS serviços que você usa.

No AWS Backup painel, você pode gerenciar planos de backup, criar backups sob demanda, restaurar backups e visualizar o status das tarefas de backup e restauração.

Tópicos

Visualizar o status dos trabalhos de backup

Use o AWS Backup painel para visualizar rapidamente o status da sua atividade de backup e restauração.

Como visualizar o status dos trabalhos de backup

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Painel.
3. Para visualizar o status de seus trabalhos de backup, escolha Detalhes dos trabalhos de backup. Isso abre a página Tarefas de backup, onde poderá visualizar tabelas que contêm trabalhos de backup e de restauração.
4. É possível filtrar os trabalhos que são exibidos por tempo. Por exemplo, trabalhos criados nas últimas 24 horas, na última semana ou nos últimos 30 dias. Você também pode definir o número de trabalhos a serem exibidos por página escolhendo o ícone de engrenagem.

Visualizar todos os backups em um cofre

Siga estas etapas para visualizar os backups que foram criados em um cofre especificado no AWS Backup.

Como visualizar todos os backups em um cofre

1. No AWS Backup console, no painel de navegação, escolha Backup vaults.
2. Escolha o cofre que você usou ao criar um backup sob demanda ou programado e visualize todos os backups que foram criados nesse cofre.

> **Note**
>
> Cada backup tem um status, que geralmente é concluído. Se, por algum motivo, não AWS Backup conseguir excluir um backup de acordo com sua configuração de ciclo de vida, ele marcará esse backup como Expirado. Você é cobrado pelo armazenamento que os backups expirados consomem e deve excluí-los.

Visualizar detalhes dos recursos protegidos

Na página Recursos protegidos, você pode explorar os detalhes dos recursos submetidos a backup no AWS Backup.

Como visualizar recursos protegidos

1. No AWS Backup console, no painel de navegação, escolha Recursos protegidos.
2. Veja os AWS recursos que estão sendo copiados. Escolha um recurso da lista para explorar seus backups associados a ele.

Próximas etapas

Para restaurar um ponto de recuperação que você visualizou, prossiga paraConceitos básicos 6: restaurar um backup.

Conceitos básicos 6: restaurar um backup

Depois que um recurso é copiado pelo menos uma vez, ele é considerado protegido e está disponível para ser restaurado usando AWS Backup. Siga estas etapas para restaurar um recurso usando o console do AWS Backup .

Para obter informações sobre parâmetros de restauração para serviços específicos ou como restaurar um backup usando a AWS CLI ou a AWS Backup API, consulte Restaurando um backup.

Como restaurar um recurso

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID do recurso que deseja restaurar.
3. Uma lista de seus pontos de recuperação, incluindo o tipo de recurso, é exibida por ID de recurso. Escolha um recurso para abrir a página Detalhes do recurso.
4. Para restaurar um recurso, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.
5. Especifique os parâmetros de restauração. Os parâmetros de restauração exibidos são específicos ao tipo de recurso selecionado.

   > **Note**
   >
   > Se você mantiver apenas um backup, só poderá restaurar o estado do sistema de arquivos no momento em que fez esse backup. Não será possível restaurar backups incrementais anteriores.

   Para obter instruções sobre como restaurar recursos específicos, consulte Restauração de um backup.
6. Para a Função de restauração, escolha Função padrão.

   > **Note**
   >
   > Se a função AWS Backup padrão não estiver presente na sua conta, uma função será criada para você com as permissões corretas.
7. Escolha Restaurar backup.

O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.

> **Note**
>
> Ao executar uma restauração para itens específicos em uma instância do Amazon EFS, você poderá restaurar esses itens em um sistema de arquivos novo ou existente. Se você restaurar os itens em um sistema de arquivos existente, AWS Backup cria um novo diretório Amazon EFS fora do diretório raiz para conter os itens. A hierarquia completa dos itens especificados é preservada no diretório de recuperação. Por exemplo, se o diretório A contiver os subdiretórios B, C e D, AWS Backup manterá a estrutura hierárquica quando A, B, C e D forem recuperados.
>
> Independentemente de você executar uma restauração parcial do Amazon EFS em um sistema de arquivos existente ou em um novo sistema de arquivos, cada tentativa de restauração criará um diretório de recuperação fora do diretório raiz para conter os arquivos restaurados. Se você tentar várias restaurações para o mesmo caminho, poderão existir vários diretórios contendo os itens restaurados.

Como restaurar uma instância do EFS

Se estiver restaurando uma instância do Amazon EFS, você poderá executar uma Restauração completa, que restaura todo o sistema de arquivos. Ou você poderá restaurar arquivos e diretórios específicos usando a restauração em nível de item (as restaurações em nível de item têm limites. Consulte Restaurar um sistema de arquivos do EFS para obter mais informações). Para obter informações sobre como restaurar outros tipos de recursos, consulte Restaurar um backup.

> **Note**
>
> Para restaurar uma instância do Amazon EFS, você deverá “Permitir” o `backup:startrestorejob`.

Para obter informações detalhadas sobre restauração de um backup, consulte Restaurar um backup.

Próximas etapas

Com o AWS Backup Audit Manager, você pode auditar sua atividade e seus recursos de backup. Também é possível criar relatórios que podem ser usados como evidência de seus trabalhos de backup, restauração e cópia. Para criar um relatório, consulte Conceitos básicos 7: criar um relatório de auditoria.

Conceitos básicos 7: criar um relatório de auditoria

EmConceitos básicos 5: visualizar suas tarefas de backup e pontos de recuperação, você observou sua atividade de backup nas visualizações AWS Backup Painel, Cofre de Backup e Recursos Protegidos. No entanto, essas visualizações são dinâmicas e serão atualizadas dependendo de quando você as acessar. Essas visualizações não são necessariamente a melhor evidência de conformidade contínua com seus requisitos e controles organizacionais de proteção de dados ao longo do tempo.

Nesta etapa, você criará um relatório de trabalho de backup sob demanda usando o AWS Backup Audit Manager.

AWS Backup O Audit Manager entrega uma variedade de relatórios de auditoria em CSV, JSON ou ambos os formatos diariamente e sob demanda para seu bucket Amazon S3. É possível auditar a conformidade de suas atividades e recursos de backup com base em vários controles personalizáveis. Você pode receber relatórios sobre suas tarefas de backup, cópia e restauração. O relatório de trabalhos de backup é uma evidência de que os trabalhos ocorreram.

Veja a seguir um exemplo de plano de backup.


```
{
  "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 criar um relatório de backup (incluindo um relatório de backup sob demanda), primeiro crie um plano de relatório para automatizar seus relatórios e fornecê-los a um bucket do Amazon S3.

Um plano de relatório exige que você tenha um bucket do Amazon S3 para receber seus relatórios. Para obter instruções sobre como configurar um novo bucket do S3, consulte Etapa 1: criar seu primeiro bucket do S3 no Guia do usuário do Amazon Simple Storage Service.

Como criar um plano de relatório

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Relatórios.
3. Escolha Criar plano de relatório.
4. Selecione Relatório de trabalhos de backup na lista suspensa.
5. No Nome do plano de relatório, insira **`TestBackupJobReport`**.
6. Em Formato de arquivo, escolha CSV e JSON.
7. Para o nome do bucket do S3, selecione o destino dos seus relatórios na lista suspensa.
8. Escolha Criar plano de relatório.

Em seguida, você deve permitir que seu bucket do S3 receba o relatório de AWS Backup. AWS Backup O Audit Manager gera automaticamente uma política de acesso do S3 para você.

Como visualizar e aplicar essa política de acesso

1. No painel de navegação à esquerda, escolha Relatórios.

2. Em Nome do plano de relatório, escolha o nome do seu plano de relatório (`TestBackupJobReport`).
3. Selecione a opção Editar.
4. Escolha Exibir política de acesso para o bucket do S3.
5. Escolha Copiar permissões.
6. Escolha Editar política de bucket para editar a política do bucket do S3 de destino e permitir que ele receba seus relatórios de trabalho de backup.
7. Copie ou adicione as permissões à política de bucket do S3 de destino.

Depois, crie seu primeiro relatório de trabalhos de backup.

Como criar um relatório de backups sob demanda

1. No painel de navegação à esquerda, escolha Relatórios.
2. Em Nome do plano de relatório, escolha o nome do seu plano de relatório (`TestBackupJobReport`).
3. Escolha Criar relatório de backups sob demanda.

Por fim, visualize o relatório.

Como visualizar o relatório

1. No painel de navegação à esquerda, escolha Relatórios.
2. Em Nome do plano de relatório, escolha o nome do seu plano de relatório (`TestBackupJobReport`).
3. Na seção Relatar trabalhos, escolha o link do S3. Isso direcionará você para o bucket do S3 de destino.
4. Escolha Baixar.
5. Abra o relatório por meio do programa que você usa para trabalhar com arquivos CSV ou JSON.

Próximas etapas

Para limpar seus recursos iniciais e evitar cobranças indesejadas, prossiga para Conceitos básicos 8: limpar os recursos.

Conceitos básicos 8: limpar os recursos

Depois de executar todas as tarefas no Começando com AWS Backup, você poderá limpar o que criou para evitar incorrer em cobranças desnecessárias.

Tópicos

Etapa 1: excluir AWS recursos restaurados

Para excluir AWS recursos que você restaurou de um ponto de recuperação, como volumes do Amazon Elastic Block Store (Amazon EBS) ou tabelas do Amazon DynamoDB, você usa o console desse serviço. Por exemplo, para excluir um sistema de arquivos do Amazon Elastic File System (Amazon EFS), use o console do Amazon EFS.

> **Note**
>
> Essas informações se referem aos recursos restaurados, não aos pontos de recuperação armazenados em um cofre de backup.

Etapa 2: excluir o plano de backup

Se não quiser criar backups programados, você deverá excluir seus planos de backup. Antes que possa excluir um plano de backup, você deverá excluir todas as atribuições de recursos desse plano.

Siga estas etapas para excluir um plano de backup:

Como excluir um plano de backup

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Planos de backup.

3. Na página Planos de backup, selecione o plano de backup que deseja excluir. Você será redirecionado para a página de detalhes do backup em questão.
4. Para excluir as atribuições de recurso do seu plano, escolha o botão ao lado do nome da atribuição e escolha Excluir.
5. Para excluir o plano de backup, escolha Excluir no canto superior direito da página.
6. Na página de confirmação, insira o nome do plano e escolha Excluir plano.

Etapa 3: excluir os pontos de recuperação

Você pode excluir os pontos de recuperação de backup que estão no cofre de backup.

Como excluir os pontos de recuperação

1. No AWS Backup console, no painel de navegação, escolha Backup vaults.
2. Na página Cofres de backup, escolha o cofre no qual você armazenou os backups.
3. Verifique o ponto de recuperação e escolha Excluir.
4. Se você estiver excluindo mais de um ponto de recuperação, siga estas etapas:

    a. Se a sua lista contiver um backup contínuo, escolha se deseja manter ou excluir seus dados de backup contínuo.

    b. Para excluir todos os pontos de recuperação listados, digite **`delete`** e escolha Excluir pontos de recuperação.

    Mantenha a guia do navegador aberta até que um banner de êxito verde seja exibido na parte superior da página. Fechar prematuramente essa guia encerrará o processo de exclusão e poderá deixar para trás alguns dos pontos de recuperação que você deseja excluir. Para obter mais informações, consulte Excluir backups.

Etapa 4: excluir o cofre de backup

Normalmente, não é possível excluir o cofre de backup padrão. No entanto, se um ou mais cofres estiverem presentes em uma região, o cofre de backup padrão nessa região poderá ser excluído usando a AWS CLI.

Você pode excluir outros cofres não padrão depois que todos os backups (pontos de recuperação) contidos nele tiverem sido excluídos. Para fazer isso, selecione Excluir no cofre vazio.

Etapa 5: excluir o plano de relatório

Seu plano de relatório envia automaticamente um novo relatório diariamente. Para evitar isso, exclua o plano de relatório.

Como excluir o plano de relatório

1. No AWS Backup console, no painel de navegação, escolha Relatórios.
2. Em Nome do plano de relatório, escolha o nome do seu plano de relatório.
3. Escolha Excluir.
4. Insira o nome do plano de relatório e escolha Excluir plano de relatório.

Etapa 6: excluir os relatórios

É possível excluir os relatórios seguindo as instruções para excluir um único objeto para cada um de seus relatórios. Se não precisar mais do bucket do S3 de destino, depois de excluir todos os objetos do bucket, você poderá excluir o bucket seguindo as instruções para Excluir um bucket.

Gerenciar backups usando planos de backup

Em AWS Backup, um plano de backup é uma expressão de política que define quando e como você deseja fazer backup de seus AWS recursos, como tabelas do Amazon DynamoDB ou sistemas de arquivos do Amazon Elastic File System (Amazon EFS). Você pode atribuir recursos aos planos de backup e fazer backup e reter AWS Backup automaticamente os backups desses recursos de acordo com o plano de backup. Você poderá criar vários planos de backup se tiver workloads com diferentes requisitos de backup. Por padrão, as janelas de backup são otimizadas pelo AWS Backup. É possível personalizar a janela de backup no console ou de forma programática.

AWS Backup armazena eficientemente seus backups periódicos de forma incremental. O primeiro backup de um recurso da AWS faz o backup de uma cópia completa dos seus dados. Para cada backup incremental sucessivo, somente as alterações em seus AWS recursos são copiadas. Os backups incrementais permitem que você se beneficie da proteção de dados de backups frequentes e, ao mesmo tempo, minimize os custos de armazenamento.

AWS Backup também gerencia perfeitamente o ciclo de vida do seu plano de backup com base nas configurações de retenção, o que permite que você restaure quando necessário.

As seções a seguir fornecem as noções básicas sobre como gerenciar sua estratégia de backup em AWS Backup.

Tópicos

Criar um plano de backup

Você pode criar um plano de backup usando o AWS Backup console, a API, a CLI, o SDK ou um modelo. AWS CloudFormation

Tópicos

- Opções de planos e configuração de backup
- AWS CloudFormation modelos para planos de backup

Criar planos de backup usando o console do AWS Backup

Abra o AWS Backup console em https://console.aws.amazon.com/backup. No painel, escolha Gerenciar planos de backup. Ou, usando o painel de navegação, escolha Planos de backup e Criar plano de backup.

Opções de início

Você tem três opções para um novo plano de backup:

- Etapa 1: criar um plano backup de com base em um existente
- Criar um novo plano
- Criação de planos de backup usando o AWS CLI

Neste tutorial, escolheremos Criar um novo plano. Cada parte da configuração tem um link para uma seção expandida mais adiante na página, à qual você pode navegar para obter mais detalhes.

1. Insira o nome do plano em Nome do plano de backup. Você não pode alterar o nome de um plano depois que ele é criado.

   Se você tentar criar um plano de backup idêntico a um plano existente, receberá um `AlreadyExistsException` erro.
2. Se preferir, você pode adicionar etiquetas ao plano de backup.
3. Configuração da regra de backup: na seção de configuração da regra de backup, você definirá a programação, a janela e o ciclo de vida do backup.
4. Programação:

   a. Insira um Nome da regra de backup no campo de texto.

   b. No menu suspenso do cofre de backup, escolha Padrão ou escolha Criar novo cofre de backup para criar um cofre.

   c. No menu suspenso da frequência de backup, escolha com que frequência você deseja que esse plano crie um backup.
5. Janela de backup:

a. O horário de início padrão é 12:30 AM (00:30 no horário de 24 horas) no fuso horário local do seu sistema.

b. Iniciar dentro de é padronizado como 8 horas. Você pode alterar essa opção para especificar uma janela de tempo para o início do backup.

c. Concluir dentro de é padronizado como 7 dias.

6. Backups e point-in-time restauração contínuos (PITR): Você pode selecionar Habilitar backups contínuos para point-in-time recuperação (PITR). Para verificar quais recursos são compatíveis com esse tipo de backup, consulte a matriz de Disponibilidade de recursos por recurso.

7. Ciclo de vida

a. Armazenamento frio: marque essa caixa para permitir que os tipos de recurso elegíveis façam a transição para o armazenamento frio de acordo com o cronograma especificado no período total de retenção. Para usar o armazenamento frio, você deve ter um período total de retenção de 90 dias ou mais.

b. O Armazenamento frio para Amazon EBS é o Arquivo de Snapshots do Amazon EBS. Os snapshots transferidos para o nível de armazenamento de arquivo serão exibidos no console como nível frio. Se o armazenamento frio estiver habilitado e se a frequência de backup for mensal ou inferior, você poderá fazer com que o plano de backup faça a transição dos snapshots do EBS.

c. O Período total de retenção é o número de dias em que você armazena o recurso no AWS Backup. É o número total de dias de armazenamento quente e armazenamento frio.

8. (Opcional) Use Copiar para o destino para criar uma cópia entre regiões dos recursos elegíveis se quiser armazenar uma cópia de um backup em outra Região da AWS.

9. (Opcional) Etiquetas adicionadas a pontos de recuperação.

10. Quando todas as seções estiverem definidas de acordo com as suas especificações, escolha Salvar regra de backup.

Criação de planos de backup usando o AWS CLI

Você também pode definir seu plano de backup em um documento JSON e fornecê-lo usando o console do AWS Backup ou a AWS CLI. O documento JSON a seguir contém um exemplo de plano de backup que cria um backup diário às 1:00, horário do Pacífico (o horário local se ajusta às condições do dia, padrão ou horário de verão, se aplicável). Ele exclui automaticamente um backup após um ano.

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

É possível armazenar o documento JSON com o nome de sua escolha. O comando da CLI a seguir mostra `create-backup-plan` com um JSON chamado `test-backup-plan.json`:

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

Observe que, embora alguns sistemas numerem os dias da semana de 0 a 6, nós os numeramos de 1 a 7. Para obter mais informações, consulte Expressões Cron. Para obter mais informações sobre fusos horários, consulte TimeZonea referência da API Amazon Location Service.

Opções de planos e configuração de backup

Ao definir um plano de backup no AWS Backup console, você configura as seguintes opções:

Nome do plano de backup

Você deve fornecer um nome exclusivo para o plano de backup.

Se escolher um nome que seja idêntico ao nome de um plano existente, você receberá uma mensagem de erro.

Regras de backup

Os planos de backup contêm uma ou mais regras de backup. Como adicionar regras de backup a um plano de backup ou editar regras existentes em um plano de backup:

1. No AWS Backup console, no painel de navegação esquerdo, escolha Planos de backup.
2. Em Nome do plano de backup, selecione um plano de backup.
3. Na seção Regras de backup:
   - Para adicionar uma regra de backup, escolha Adicionar regra de backup.
   - Para editar uma regra de backup existente, selecione a regra e Editar regra.

> **Note**
>
> Se você tem um plano de backup com várias regras e os prazos das duas regras se sobrepõem, AWS Backup otimiza o backup e faz um backup da regra com maior tempo de retenção. A otimização leva em consideração a janela inicial completa, não apenas quando o backup diário é feito.

Cada regra de backup consiste nos elementos a seguir.

Nome da regra de backup

Os nomes das regras de backup fazem distinção de maiúsculas de minúsculas. Devem conter de 1 a 50 caracteres alfanuméricos ou hífens.

Frequência de Backup

A frequência do backup determina a frequência com que um backup instantâneo é AWS Backup criado. Usando o console, é possível escolher uma frequência de a cada hora, a cada 12 horas, diária, semanal ou mensal. Também é possível criar uma expressão cron que crie backups de snapshot com a frequência de a cada hora. Usando a AWS Backup CLI, você pode programar backups de instantâneos com a mesma frequência de hora em hora.

Ao selecionar a frequência semanal, você pode especificar os dias da semana em que deseja que os backups sejam feitos. Ao selecionar a frequência mensal, você pode escolher um determinado dia do mês.

Você também pode marcar a caixa de seleção Habilitar backups contínuos para recursos suportados para criar uma regra de backup contínuo habilitada para point-in-time restauração (PITR). Diferentemente dos backups instantâneos, os backups contínuos permitem que você realize a point-in-time restauração. Para saber mais sobre backups contínuos, consulte Recuperação para um ponto no tempo.

Janela de backup

As janelas de backup consistem na hora em que a janela de backup começa e na duração da janela em horas. Os trabalhos de backup são iniciados nessa janela. As configurações padrão no console são:

- 12:30 AM local do fuso horário do seu sistema (0:30 em sistemas de 24 horas)
- Começar em 8 horas
- Concluir em 7 dias

  (O parâmetro Concluir dentro de não se aplica aos recursos do Amazon FSx.)

É possível personalizar a frequência de backups e o horário de início da janela de backup usando uma expressão cron. Para ver os seis campos das expressões AWS cron, consulte Expressões cron no Guia do usuário do Amazon CloudWatch Events. Dois exemplos de expressões AWS cron são `15 * ? * * *` (faça um backup a cada hora, 15 minutos após a hora) e `0 12 * * ? *` (faça um backup todos os dias às 12h UTC). Para ver uma tabela de exemplos, clique no link anterior e role a página para baixo.

AWS Backup avalia expressões cron entre 00:00 e 23:59. Se você criar uma regra de backup “a cada 12 horas”, mas fornecer um horário de início posterior às 11:59, ela será executada somente uma vez por dia.

Os backups e point-in-time restaurações contínuos (PITR) fazem referência às alterações registradas em um período de tempo; portanto, eles não podem ser programados com uma expressão de hora ou cron.

> **Note**
>
> Em geral, os serviços AWS de banco de dados não podem iniciar os backups 1 hora antes ou durante a janela de manutenção e o Amazon FSx não pode iniciar os backups 4 horas antes ou durante a janela de manutenção ou a janela de backup automático (o Amazon

Aurora está isento dessa restrição da janela de manutenção). haverá falha nos backups de snapshot programados durante esses horários.
Uma exceção ocorre quando você opta por usar o AWS Backup para backups de snapshot e backups contínuos de um serviço compatível. O AWS Backup programará janelas de backup automaticamente para evitar conflitos. Consulte Point-in-Time Recovery para obter uma lista de serviços suportados e instruções sobre como usar AWS Backup para fazer backups contínuos.

Regras de backup sobrepostas

Ocasionalmente, um plano de backup pode conter várias regras sobrepostas. Quando as janelas iniciais de regras diferentes se sobrepõem, AWS Backup retém o backup sob a regra com o período de retenção mais longo. Por exemplo, considere um plano de backup com duas regras:

1. Fazer backup a cada hora, com uma janela de início de uma hora, e reter por um dia.
2. Fazer backup a cada 12 horas, com uma janela de início de oito horas, e reter por uma semana.

Depois de 24 horas, a segunda regra cria dois backups (porque tem um período de retenção mais longo). A primeira regra cria oito backups (porque a janela de início de oito horas da segunda regra impediu a execução de mais backups por hora). Especificamente:

Durante esta janela de início	Esta regra cria um backup
Meia-noite às 8h	12 horas
de 8 às 9	Por hora
de 9 às 10	Por hora
de 10 às 11	Por hora
de 11 ao meio-dia	Por hora
Do meio-dia às 20h	12 horas
de 8 às 9	Por hora
de 9 às 10	Por hora

Durante esta janela de início	Esta regra cria um backup
de 10 às 11	Por hora
de 11 à meia-noite	Por hora

Durante a janela inicial, o status da tarefa de backup permanece no status `CREATED` até que seja iniciado com sucesso ou até que o tempo da janela de início se esgote. Se, dentro da janela inicial, o horário AWS Backup receber um erro que permita que o trabalho seja repetido, AWS Backup tentará iniciá-lo automaticamente pelo menos a cada 10 minutos até que o backup seja iniciado com sucesso (o status do trabalho mude para`RUNNING`) ou até que o status do trabalho mude para `EXPIRED` (o que se espera que ocorra quando o tempo da janela inicial terminar).

Ciclo de vida e níveis de armazenamento

Os backups são armazenados pelo número de dias que você especificar, o que é conhecido como ciclo de vida do backup. Os backups podem ser restaurados até o final de seu ciclo de vida.

Isso é definido como o período total de retenção na seção do ciclo de vida da configuração da regra de backup no AWS Backup console.

Se você usa AWS CLI, isso é definido usando o parâmetro `DeleteAfterDays`. O período de retenção para snapshots pode variar entre um dia e 100 anos (ou indefinidamente se você não inserir um valor), enquanto o período de retenção para backups contínuos pode variar de um dia a 35 dias. A data de criação de um backup é a data em que a tarefa de backup começou, não a data em que foi concluída. Se sua tarefa de backup não for concluída na mesma data em que começou, use a data em que ela começou para ajudar a calcular os períodos de retenção.

Os backups são mantidos em um nível de armazenamento. Cada nível tem um custo diferente de armazenamento e restauração, conforme descrito nos Preços do AWS Backup. Cada backup é criado e armazenado em um armazenamento quente. Dependendo do tempo que você decidir armazenar o backup, talvez queira fazer a transição do backup para um nível de menor custo chamado armazenamento frio. O Disponibilidade de recursos por recurso exibe quais recursos têm essa opção.

Console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.

2. Crie ou edite um plano de backup.
3. Na seção do ciclo de vida da configuração da regra de backup, marque a caixa Mova os backups do armazenamento quente para o armazenamento frio.
4. (Opcional) Se o Amazon EBS for um dos recursos que você faz backup e a frequência de backup for mensal ou inferior, você poderá transferi-los para o nível frio usando o arquivamento de snapshots do EBS.
5. Insira um valor (em dias) em que você deseja que seus backups permaneçam em um armazenamento aquecido. AWS Backup recomenda pelo menos 8 dias.
6. Insira um valor (em dias) para o período total de retenção. A diferença entre o período total de retenção e o tempo em armazenamento quente será a quantidade de dias em que os backups permanecerão no armazenamento frio.

AWS CLI

1. Use `create-backup-plan` ou `update-backup-plan`.
2.
3. Inclua o parâmetro booleano `OptInToArchiveForSupportedResources` para recursos do EBS.
4. Inclua o parâmetro `MoveToColdStorageAfterdays`.
5. Use o parâmetro `DeleteAfterDays`. Esse valor deve ser 90 (dias) mais o valor que você inseriu para `MoveToColdStorageAfterDays`.

No momento, o armazenamento frio está disponível para os seguintes tipos de recurso:

Tipo de recurso	Backup incremental ou completo em armazenamento frio
AWS CloudFormation	Incremental
DynamoDB com recursos avançados do	Completo; sem backups incrementais em nenhum nível
Amazon EBS (usando o Arquivo de Snapshots do EBS)	Completo; os backups incrementais se tornarão completos após a transição

Tipo de recurso	Backup incremental ou completo em armazenamento frio
Amazon EFS	Incremental
Bancos de dados SAP HANA em instâncias do Amazon EC2	Incremental
Amazon Timestream	Incremental
Máquinas virtuais da VMware	Incremental

Depois de habilitar a transição para o armazenamento frio por meio do console ou da linha de comandos, as seguintes condições serão verdadeiras para backups em armazenamento frio (ou arquivamento):

- Os backups transferidos devem ser armazenados em armazenamento frio por no mínimo 90 dias, além do tempo em armazenamento quente. AWS Backup exige que a retenção seja definida por 90 dias a mais do que a configuração de “transição para o frio após dias”. Não é possível alterar a configuração do "número de dias para transição para armazenamento frio"' depois que a transição para "frio" foi habilitada.
- Alguns serviços oferecem suporte a backups incrementais. Para backups incrementais, você deve ter pelo menos um backup completo a quente. AWS Backup recomenda que você defina suas configurações de ciclo de vida para não mover seu backup para o armazenamento refrigerado até pelo menos 8 dias. Se o backup completo for transferido para o armazenamento frio muito cedo (por exemplo, uma transição para o armazenamento frio após 1 dia), AWS Backup criará outro backup completo a quente.
- Para tipos de recursos que oferecem suporte a backups incrementais, AWS Backup faz a transição dos dados do armazenamento quente para o armazenamento frio se os dados da transição não forem mais referenciados pelos backups quentes. Os dados em backups retidos em armazenamento frio que são referenciados somente por outros backups frios são cobrados de acordo com os preços do nível de armazenamento frio. Outros backups continuam com preços do nível de armazenamento quente.

Cofre de backup

Um cofre de backup é um contêiner no qual organizar seus backups. Os backups criados por uma regra de backup são organizados no cofre de backup que você especifica na regra de backup. Você pode usar cofres de backup para definir a chave de criptografia AWS Key Management Service (AWS KMS) usada para criptografar backups no cofre de backup e controlar o acesso aos backups no cofre de backup. Também é possível adicionar tags a cofres de backup para ajudar a organizá-los. Se não quiser usar o cofre padrão, você poderá criar o seu próprio cofre. Para step-by-step obter instruções sobre como criar um cofre de backup, consulteEtapa 3: criar um cofre de backup.

Copiar em regiões

Como parte do plano de backup, você pode, opcionalmente, criar uma cópia de backup em outra Região da AWS. Para obter mais informações sobre cópias de backup, consulte Criar cópias de backup em Regiões da AWS.

Ao definir uma cópia de backup, você configura as seguintes opções:

Região de destino

A região de destino da cópia de backup.

(Configurações avançadas) Cofre de backup

O cofre de backup de destino da cópia.

(Configurações avançadas) Perfil do IAM

A função do IAM AWS Backup usada ao criar a cópia. A função também deve estar AWS Backup listada como uma entidade confiável, o que AWS Backup permite assumir a função. Se você escolher Padrão e a função AWS Backup padrão não estiver presente na sua conta, uma função será criada para você com as permissões corretas.

(Configurações avançadas) Ciclo de vida

Especifica quando fazer a transição da cópia de backup para armazenamento estático e quando expirar (excluir) a cópia. Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Você não poderá alterar esse valor depois que a transição da cópia for feita para o armazenamento estático.

Expirar especifica o número de dias em que a cópia é excluída depois de sua criação. O número de dias deve ser superior a 90 dias além do valor da Transição para armazenamento estático.

Tags adicionadas a pontos de recuperação

As tags que você listar aqui serão automaticamente adicionadas aos backups quando eles forem criados.

Tags adicionadas aos planos de backup

Essas tags são associadas ao plano de backup em si, para ajudar você a organizar e acompanhar o plano de backup.

Configurações avançadas de backup

Habilita backups consistentes de aplicações de terceiros que estão em execução em instâncias do Amazon EC2. Atualmente, AWS Backup oferece suporte a backups do Windows VSS. AWS Backup exclui tipos específicos de instância do Amazon EC2 dos backups do Windows VSS. Para ter mais informações, consulte Criar backups do VSS do Windows.

AWS CloudFormation modelos para planos de backup

Nós fornecemos dois AWS CloudFormation modelos de amostra para sua referência. O primeiro modelo cria um plano de backup simples. O segundo modelo permite backups do VSS em um plano de backup.

> **Note**
>
> Se você estiver usando o perfil de serviço padrão, substitua o *perfil de serviço* 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
```

Atribuir recursos a um plano de backup

A atribuição de recursos especifica quais recursos AWS Backup serão protegidos usando seu plano de backup. AWS Backup oferece configurações padrão simples e controles refinados para atribuir recursos ao seu plano de backup. Sempre que seu plano de backup é executado, ele examina todos Conta da AWS os recursos que correspondem aos seus critérios de atribuição de recursos. Esse nível de automação permite que você defina seu plano de backup e a atribuição de recursos exatamente uma vez. AWS Backup resume o trabalho de encontrar e fazer backup de novos recursos adequados à sua atribuição de recursos definida anteriormente.

Você pode atribuir qualquer tipo de recurso AWS Backup compatível que você tenha optado por AWS Backup gerenciar. Para obter instruções sobre como optar por mais tipos AWS Backup de recursos compatíveis, consulte Introdução 1: Opção de serviço.

O AWS Backup console tem duas maneiras de incluir tipos de recursos em um plano de backup: atribuir explicitamente o tipo de recurso em um plano de backup ou incluir todos os recursos. Veja os pontos abaixo para entender como essas seleções funcionam com as inclusões no serviço.

- Se as atribuições de recursos forem baseadas somente em tags, as configurações de inclusão no serviço serão aplicadas.
- Se um tipo de recurso for explicitamente atribuído a um plano de backup, ele será incluído no backup mesmo que o opt-in não esteja habilitado para esse serviço específico. Isso não se aplica ao Aurora, ao Neptune e ao Amazon DocumentDB. Para que esses serviços sejam incluídos, o opt-in deve estar ativado.
- Se o tipo de recurso e as tags forem especificados em uma atribuição de recurso, os tipos de recursos especificados serão filtrados primeiro e, em seguida, as tags filtrarão ainda mais esses recursos.

  As configurações de aceitação do serviço são ignoradas na maioria dos tipos de recursos. No entanto, o Aurora, o Neptune e o Amazon DocumentDB exigem a aceitação do serviço.
- Quando uma conta usa AWS Backup (cria um cofre de backup ou um plano de backup) em uma região, a conta é automaticamente incluída em todos os tipos de recursos suportados pela AWS Backup região naquele momento. Os serviços suportados adicionados a essa região posteriormente não serão incluídos automaticamente em um plano de backup. Você pode optar por optar por esses tipos de recursos assim que eles se tornarem compatíveis.
- Para o Amazon FSx for NetApp ONTAP, ao usar a seleção de recursos com base em tags, aplique tags em volumes individuais em vez de em todo o sistema de arquivos.

Sua atribuição de recursos pode incluir (ou excluir) tipos de recursos e recursos.

- Um tipo de recurso inclui cada instância ou recurso de um AWS serviço AWS Backup compatível ou aplicativo de terceiros. Por exemplo, o tipo de recurso do DynamoDB se refere a todas as suas tabelas do DynamoDB.
- Um recurso é uma instância única de um tipo de recurso, como uma de suas tabelas do DynamoDB. É possível especificar um recurso usando seu ID de recurso exclusivo.

É possível refinar ainda mais sua atribuição de recursos usando tags e operadores condicionais.

Tópicos

- Atribuir recursos usando o console

- Atribuir recursos de forma programática
- Atribuindo recursos usando AWS CloudFormation
- Cotas de atribuição de recursos

Atribuir recursos usando o console

Como navegar até a página Atribuir recursos:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Escolha planos de backup.
3. Escolha Criar plano de backup.
4. Selecione qualquer modelo na lista suspensa Escolher modelo e, em seguida, escolha Criar plano.
5. Digite um Nome de plano de backup.
6. Selecione Criar plano.
7. Selecione Atribuir recursos.

Para começar sua atribuição de recursos, na seção Geral:

1. Digite o nome de uma atribuição de recurso.
2. Escolha a Função padrão ou Escolha um perfil do IAM.

> **Note**
>
> Se você escolher um perfil do IAM, verifique se ele tem permissão para fazer backup de todos os recursos que você está prestes a atribuir. Se o perfil encontrar um recurso para o qual não tenha permissão para acessar, haverá falha.

Para atribuir seus recursos, na seção Atribuir recursos, selecione uma das duas opções em Definir seleção de recursos:

- Incluir todos os tipos de recursos. Essa opção configura seu plano de backup para proteger todos os recursos AWS Backup suportados atuais e futuros atribuídos ao seu plano de backup. Use essa opção para proteger de forma rápida e fácil seu conjunto de dados.

Ao escolher essa opção, você pode, opcionalmente, refinar a seleção usando tags como a próxima etapa.

- Incluir tipos de recursos específicos. Ao escolher essa opção, você deve selecionar tipos de recursos específicos com as seguintes etapas:

  1. Usando o menu suspenso Selecionar tipos de recursos, atribua um ou mais tipos de recursos.

     > **Important**
     >
     > O RDS, o Aurora, o Neptune e o DocumentDB compartilham o mesmo nome do recurso da Amazon (ARN). Optar por gerenciar um desses tipos de recursos com o AWS Backup inclui todos eles ao atribuí-lo a um plano de backup. Para refinar sua seleção, use tags e operadores condicionais.

     Ao terminar, AWS Backup apresenta a lista dos tipos de recursos selecionados e sua configuração padrão, que é proteger todos os recursos de cada tipo de recurso selecionado.

  2. Opcionalmente, se você quiser excluir recursos específicos de um tipo de recurso selecionado:

     1. Use o menu suspenso Escolher recursos e desmarque a opção padrão.
     2. Selecione os recursos específicos a serem atribuídos ao seu plano de backup.

  3. Opcionalmente, é possível Excluir IDs de recursos específicos dos tipos de recursos selecionados. Use essa opção se quiser excluir um ou alguns recursos de muitos, pois isso pode ser mais rápido do que selecionar muitos recursos durante a etapa anterior. Você deve incluir um tipo de recurso antes de excluir recursos desse tipo de recurso. Exclua uma ID de recurso usando as seguintes etapas:

     1. Em Excluir IDs de recursos específicos dos tipos de recursos selecionados, escolha um ou mais dos tipos de recursos que você incluiu usando Selecionar tipos de recursos.
     2. Para cada tipo de recurso, use o menu Escolher recursos para selecionar um ou mais recursos a serem excluídos.

Além das escolhas anteriores, é possível fazer seleções ainda mais granulares usando o recurso opcional Refinar seleção usando tags. Esse recurso permite que você refine sua seleção atual para incluir um subconjunto de seus recursos usando tags.

As tags são pares de chave/valor que podem ser atribuídas a recursos específicos para ajudar você a identificar, organizar e filtrar seus recursos. As tags diferenciam letras maiúsculas de minúsculas. Para obter mais informações, consulte Marcar recursos da AWS na Referência geral da AWS .

Quando você refina sua seleção usando duas ou mais tags, o efeito é uma condição AND. Por exemplo, se refinar sua seleção usando duas tags, `env: prod` e `role: application`, você só atribuirá recursos com AMBAS as tags ao seu plano de backup.

Como refinar sua seleção usando tags:

1. Em Refinar seleção usando tags, escolha uma Chave na lista suspensa.
2. Escolha uma Condição para o valor na lista suspensa.
   - O valor se refere à próxima entrada, o valor do seu par de chave/valor.
   - A condição pode ser `Equals`, `Contains`, `Begins with`, `Ends with` ou seu inverso: `Does not equal`, `Does not contain`, `Does not begin with` ou `Does not end with`.
3. Escolha um Valor na lista suspensa.
4. Para refinar ainda mais usando outra tag, escolha Adicionar tag.

Atribuir recursos de forma programática

É possível definir uma atribuição de recursos em um documento JSON. Esse exemplo de atribuição de recursos atribui todas as instâncias do Amazon EC2 ao plano de backup *`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/*"
    ]
  }
}
```

Supondo que esse JSON esteja armazenado como `backup-selection.json`, você poderá atribuir esses recursos ao seu plano de backup usando o seguinte comando da CLI:

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

Veja a seguir exemplos de atribuições de recursos, junto com o documento JSON correspondente. Para facilitar a leitura dessa tabela, os exemplos omitem os campos `"BackupPlanId"`, `"SelectionName"`, e `"IamRoleArn"`. O curinga `*` representa zero ou mais caracteres que não sejam espaços em branco.

Example Exemplo: Selecionar todos os recursos em minha conta

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

Example Exemplo: selecionar todos os recursos em minha conta, mas excluir volumes do EBS

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

Example Exemplo: selecione todos os recursos marcados com"backup":"true", mas exclua os volumes do EBS

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
```

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

Example Exemplo: selecione todos os volumes do EBS e instâncias de banco de dados do RDS marcados com ambos e "backup":"true""stage":"prod"

A aritmética booleana é semelhante à das políticas do IAM, com aquelas em "Resources" combinadas usando um OR booliano e aquelas em `"Conditions"` combinadas com um AND booliano.

A expressão `"arn:aws:rds:*:*:db:*"` de `"Resources"` seleciona somente instâncias de banco de dados do RDS porque não há recursos do Aurora, Neptune ou DocumentDB correspondentes.

```
{
  "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 Exemplo: Selecione todos os volumes do EBS e instâncias do RDS marcados com"backup":"true", mas não "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 Exemplo: selecione todos os recursos marcados com "key1" e um valor que comece com"include", mas não com, "key2" e um valor que contenha a palavra "exclude"

Você pode usar o caractere curinga no início, no final e no meio de uma string. Observe o uso do caractere curinga (*) no `include*` e `*exclude*` no exemplo acima. Você também pode usar o caractere curinga no meio de uma string, conforme mostrado no exemplo anterior, `arn:aws:rds:*:*:db:*`.

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

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

Example Exemplo: Selecione todos os recursos marcados com, "backup":"true" exceto sistemas de arquivos FSx e recursos do RDS, Aurora, Neptune e DocumentDB

Os itens em `NotResources` são combinados usando o booliano OR.

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

Example Exemplo: selecione todos os recursos marcados com uma tag "backup" e qualquer valor

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

Example Exemplo: selecione todos os sistemas de arquivos FSx, o cluster Aurora e todos os recursos marcados com "my-aurora-cluster""backup":"true", exceto os recursos marcados com "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 Exemplo: Selecione todos os recursos marcados com a tag**`"backup":"true"`**, exceto os volumes do EBS marcados com **`"stage":"test"`**

Use dois comandos da CLI para criar duas seleções para selecionar esse grupo de recursos. A primeira seleção se aplica a todos os recursos, exceto aos volumes do EBS. A segunda seleção se aplica aos volumes do 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"
        }
      ]
    }
  }
}
```

Atribuindo recursos usando AWS CloudFormation

Esse end-to-end AWS CloudFormation modelo cria uma atribuição de recursos, um plano de backup e um cofre de backup de destino:

- Um cofre de backup chamado *`CloudFormationTestBackupVault`*.
- Um plano de backup chamado *`CloudFormationTestBackupPlan`*. Esse plano conterá duas regras de backup, ambas fazendo backups diariamente às 12h UTC e os retendo por 210 dias.
- Uma seleção de recursos chamada *`BackupSelectionName`*.
- • A atribuição de recursos faz backup dos seguintes recursos:
  - Qualquer recurso marcado com o par de chave/valor `backupplan:dsi-sandbox-daily`.
  - Qualquer recurso marcado com o valor `prod` ou valores que começam com `prod/`.
  - A atribuição de recursos não faz backup dos seguintes recursos:
    - Qualquer cluster do RDS, Aurora, Neptune ou DocumentDB.
    - Qualquer recurso marcado com o valor `test` ou valores que começam com `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/*
```

Cotas de atribuição de recursos

As cotas a seguir se aplicam a uma atribuição de recurso único:

- 500 Nomes de recurso da Amazon (ARNs) sem curingas
- 30 ARNs com expressões curinga
- 30 condições
- 30 tags por atribuição de recurso (e um número ilimitado de recursos por tag)

Excluir um plano de backup

Você pode excluir um plano de backup somente depois que todas as seleções de recursos associadas forem excluídas. Essas seleções também são conhecidas como atribuições de recursos. Se eles não tiverem sido excluídos antes da exclusão do plano de backup, o console exibirá o erro: “As seleções relacionadas do plano de backup devem ser excluídas antes da exclusão do plano de backup”. Use o console ou use `DeleteBackupSelection`.

A exclusão de um plano de backup exclui a versão atual do plano. As versões atuais e anteriores, se houver, ainda existem, mas elas não estão mais listadas no console em Planos de backup.

> **Note**
>
> Quando um plano de backup é excluído, os backups existentes não são excluídos. Para remover os backups existentes, exclua-os do cofre de backup usando as etapas em Excluir backups.

Para excluir um plano de backup usando o AWS Backup console

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação no lado esquerdo, selecione Planos de backup.
3. Selecione seu plano de backup na lista.
4. Selecione todas as atribuições de recursos associadas ao plano de backup.
5. Escolha Excluir.

Atualizar um plano de backup

Depois de criar um plano de backup, você pode editar o plano, por exemplo, você pode adicionar tags ou pode adicionar, editar ou excluir regras de backup. Qualquer alteração feita em um plano de backup não têm efeito sobre os backups existentes criados pelo plano de backup. As alterações se aplicam apenas a backups criados posteriormente.

Por exemplo, depois que você atualizar o período de retenção em uma regra de backup, o período de retenção de backups criados antes da atualização permanece o mesmo. Todos os backups já criados por essa regra e os próximos refletem o período de retenção.

Você não pode alterar o nome de um plano depois que ele é criado.

Para editar um plano de backup usando o AWS Backup console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Planos de backup.
3. No segundo painel, Planos de backup, os planos anteriores existentes são exibidos. Selecione o link sublinhado na coluna Nome do plano de backup para ver detalhes do plano de backup escolhido.

4. Você pode editar uma regra de backup, visualizar atribuições de recursos, visualizar tarefas de backup, gerenciar tags ou alterar as configurações do Windows VSS.
5. Para atualizar uma regra de backup, selecione o nome da regra de backup.

   Selecione Gerenciar tags para adicionar ou excluir tags.

   Selecione Editar ao lado de Configurações avançadas de backup para ativar ou desativar o Windows VSS.
6. Altere as configurações de sua preferência e selecione Salvar.

Cofres de backup

> **Note**
>
> A partir de 9 de agosto de 2023, AWS Backup está oferecendo uma prévia do uso de um cofre logicamente fechado. Para se inscrever nessa prévia, envie uma solicitação por e-mail para <aws-backup-vault-preview@amazon .com>.
> Os recursos poderão ser alterados ou ajustados durante e após o período de pré-visualização. Quando o serviço se tornar disponível para o público em geral (GA), os dados e as configurações fornecidos durante a pré-visualização não estarão mais disponíveis. A AWS recomenda usar dados de teste em vez de dados de produção com a pré-visualização.

Em AWS Backup, um cofre de backup é um contêiner que armazena e organiza seus backups.

Ao criar um cofre de backup, você deve especificar a chave de criptografia AWS Key Management Service (AWS KMS) que criptografa alguns dos backups colocados nesse cofre. A criptografia para outros backups é gerenciada por seus AWS serviços de origem. Para obter mais informações sobre a criptografia, consulte Criptografia de backups na AWS.

Sua conta sempre terá um cofre de backup padrão. Se precisar de diferentes chaves de criptografia ou políticas de acesso para diferentes grupos de backups, é possível criar vários cofres de backup.

Esta seção fornece uma visão geral de como gerenciar os cofres de backup no AWS Backup.

Tópicos

Cofres logicamente isolados (pré-visualização)

> **Note**
>
> A partir de 9 de agosto de 2023, AWS Backup está oferecendo uma prévia do uso de um cofre logicamente fechado. Para se inscrever nessa prévia, envie uma solicitação por e-mail para <aws-backup-vault-preview@amazon .com>.
> Os recursos poderão ser alterados ou ajustados durante e após o período de pré-visualização. Quando o serviço se tornar disponível para o público em geral (GA), os dados e as configurações fornecidos durante a pré-visualização não estarão mais disponíveis. A AWS recomenda usar dados de teste em vez de dados de produção com a pré-visualização.

Visão geral

AWS Backup está visualizando um tipo secundário de cofre que pode armazenar cópias de backups em outros cofres. Um cofre logicamente isolado é um cofre especializado que oferece recursos de segurança avançados, além dos de um cofre de backup, bem como a capacidade de compartilhar o acesso ao cofre com outras contas e organizações para que o tempo de recuperação (RTO) seja mais rápido e flexível no caso de um incidente que exija a restauração rápida de recursos.

Logicamente, os cofres com lacunas de ar são equipados com recursos de proteção adicionais: cada um desses cofres é criptografado com uma chave AWS própria e cada cofre tem uma trava de cofre configurada no modo de conformidade.

Você pode optar por compartilhar um cofre logicamente isolado entre organizações e contas para que os backups armazenados nele possam ser isolados a partir de uma conta com a qual o cofre é compartilhado, se necessário.

Não há cobranças adicionais pelo armazenamento em cofres logicamente isolados durante o período de pré-visualização. Os backups em cofres de backup padrão e as cópias entre regiões ainda serão cobrados de acordo com as taxas publicadas (consulte a definição de preço), embora nenhuma cópia desses backups em cofres logicamente isolados não seja cobrada.

Caso de uso

Um cofre logicamente isolado é um cofre secundário que serve como parte de uma estratégia de proteção de dados. Esse cofre pode ajudar a aprimorar sua retenção e recuperação organizacionais quando você deseja um cofre para seus backups que:

- Seja configurado automaticamente com um bloqueio de cofre no modo de conformidade
- Contenha backups que possam ser compartilhados e restaurados em uma conta diferente daquela que criou o backup
- Vem criptografado com uma AWS chave própria

Os recursos compatíveis em um cofre logicamente isolado incluem:

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

Essa pré-visualização de cofres logicamente isolados só está disponível na região Leste dos EUA (Norte da Virgínia). Como esse recurso está atualmente somente em uma região, a cópia entre regiões não será compatível durante esse período de pré-visualização.

Comparar e contrastar com um cofre de backup padrão

Um cofre de backup é o tipo principal e padrão de cofre usado em. AWS Backup Cada backup é armazenado em um cofre de backup quando o backup é criado. Você pode atribuir políticas baseadas em recursos para gerenciar backups armazenados no cofre, como o ciclo de vida dos backups armazenados no cofre.

Um cofre logicamente isolado é um cofre especializado com segurança adicional e compartilhamento flexível para um tempo de recuperação (RTO) mais rápido. Esse cofre armazena cópias de backups que foram inicialmente criadas e armazenadas em um cofre de backup padrão.

Os cofres de backup podem ser criptografados com uma chave, um mecanismo de segurança que limita o acesso aos usuários pretendidos. Essas chaves podem ser gerenciadas ou AWS gerenciadas pelo cliente. Além disso, um cofre de backup pode ser ainda mais protegido por um bloqueio de cofre. Os cofres logicamente isolados são equipados com um bloqueio de cofre no modo de conformidade.

Se a AWS KMS chave não tiver sido alterada manualmente ou definida como uma chave gerenciada pelo cliente (CMK) no momento em que o recurso inicial foi criado, um backup não poderá ser copiado em um cofre logicamente isolado.

Atributo	Cofre de backup	Cofre logicamente isolado (pré-visualização)
Criação de backup	Quando um backup é criado, ele é armazenado como um ponto de recuperação	Os backups não são armazenados neste cofre após a criação
O armazenamento do backup	Pode armazenar backups iniciais de recursos e cópias de backups	Pode armazenar cópias de backups de outros cofres
Segurança	Opcionalmente, pode ser criptografado com uma chave (gerenciada ou AWS gerenciada pelo cliente) Opcionalmente, pode ser bloqueado com um bloqueio de cofre	É criptografado com uma AWS chave própria Está sempre bloqueado com um bloqueio de cofre no modo de conformidade
Capacidade de compartilhamento	O acesso pode ser gerenciado por meio de políticas e pelo AWS Organizations Não compatível com AWS Resource Access Manager	Opcionalmente, pode ser compartilhado entre contas usando o AWS RAM
Restauração	Os backups podem ser restaurados pela mesma conta proprietária do cofre	Os backups podem ser restaurados por uma conta diferente daquela que é proprietária do backup, se o cofre for compartilhado com essa conta separada.
Regionalidade	Disponível em todas as regiões em que AWS Backup opera	Disponível na região Leste dos EUA (Norte da Virgínia) durante a pré-visualização

Atributo	Cofre de backup	Cofre logicamente isolado (pré-visualização)
Recursos	Pode armazenar backups que contêm todos os recursos AWS Backup suportados	Pode armazenar backups que contenham dados do Amazon EC2, Amazon EBS, Amazon EFS, Amazon S3 ou Amazon RDS

Criar um cofre logicamente isolado no console

> **Important**
>
> Depois que o cofre for criado, o nome do cofre, o tipo do cofre e os períodos mínimo e máximo de retenção não poderão ser alterados. Além disso, o bloqueio do cofre não poderá ser removido.
> Quando o serviço se tornar disponível ao público em geral, os dados e as configurações fornecidos durante a pré-visualização não estarão mais disponíveis. AWS recomenda usar dados de teste em vez de dados de produção com a visualização prévia.

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Configurações.
3. Os dois tipos de cofres serão exibidos. Selecione Criar cofre.
4. Insira um nome para o cofre de backup. Você pode nomear o cofre para refletir o que será armazenado nele ou para facilitar a pesquisa de backups necessários. Por exemplo, você pode nomeá-lo como: `FinancialBackups`.
5. Selecione o botão de opção para um cofre logicamente isolado.
6. Defina o período mínimo de retenção.

   Esse valor (em dias, meses ou anos) é o menor tempo em que um backup poderá ser retido nesse cofre. Backups com períodos de retenção menores que esse valor não poderão ser copiados nesse cofre.
7. Defina o período máximo de retenção.

Esse valor (em dias, meses ou anos) é a maior quantidade de tempo que um backup poderá ser retido nesse cofre. Backups com períodos de retenção maiores que esse valor não poderão ser copiados nesse cofre.

8. (Opcional) Adicione tags que ajudarão você a pesquisar e identificar seu cofre logicamente isolado. Por exemplo, você pode adicionar uma tag `BackupType:Financial`.
9. Selecione Criar cofre.
10. Reveja as configurações. Se todas as configurações forem exibidas conforme pretendido, selecione Criar um cofre logicamente isolado.
11. O console levará você à página de detalhes do novo cofre. Verifique se os detalhes do cofre estão conforme o esperado.

Visualizar detalhes de um cofre logicamente isolado no console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, selecione Pilhas.
3. Abaixo das descrições dos cofres, haverá duas listas: Cofres de propriedade dessa conta e Cofres compartilhados com essa conta. Selecione a guia desejada para ver os cofres.
4. Em Nome do cofre, clique no nome do cofre para abrir a página de detalhes. Você poderá ver o resumo, os pontos de recuperação, os recursos protegidos, o compartilhamento da conta, a política de acesso e os detalhes da tag.

Copiar de um cofre de backup padrão para um cofre logicamente isolado no console

Os cofres logicamente isolados só podem ser um destino de trabalhos de cópia em um plano de backup ou um destino para um trabalho de cópia sob demanda.

Para iniciar um trabalho de cópia, você deve ter

- Um cofre de backup
- Um cofre logicamente isolado
- Um backup contendo dados do Amazon EC2, Amazon EBS, Amazon RDS, Amazon S3 ou Amazon EFS
- A permissão `kms:CreateGrant` para a função que está sendo usada para criar a cópia.

- Sem backups criptografados com uma chave AWS gerenciada como parte de seu trabalho de cópia para o cofre logicamente fechado

Depois de confirmar os itens acima,

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, selecione Pilhas.
3. Na página de detalhes do cofre, todos os pontos de recuperação dentro desse cofre serão exibidos. Coloque uma marca de seleção ao lado do ponto de recuperação que você deseja copiar.
4. Em seguida, escolha Ações e selecione Editar no menu suspenso.
5. Na próxima tela, insira os detalhes do destino.
    a. A região deve ser definida como Leste dos EUA (Norte da Virgínia)
    b. O menu suspenso do cofre de backup de destino exibirá os cofres de destino elegíveis. Selecione um com o tipo `logically air-gapped vault`
6. Selecione Copiar quando todos os detalhes estiverem definidos de acordo com suas preferências.

Na página Trabalhos no console, você poderá selecionar trabalhos de Cópia para ver os trabalhos de cópia atuais.

Para obter mais informações, consulte Copiar um backup, Backup entre regiões e Backup entre contas.

Compartilhar um cofre logicamente isolado pelo console

> **Note**
>
> Somente as contas com determinados privilégios do IAM podem compartilhar e gerenciar o compartilhamento de contas.

Você pode usar AWS RAM para compartilhar um cofre logicamente isolado com outras contas que você designar. Para compartilhar usando AWS RAM, verifique se você tem o seguinte:

- Duas ou mais contas que podem acessar AWS Backup

- Uma conta que pretende compartilhar tem as permissões da RAM necessárias. A permissão `ram:CreateResourceShare` é necessária para esse procedimento. A política `AWSResourceAccessManagerFullAccess` contém todas as permissões necessárias relacionadas à RAM.
- Pelo menos um cofre logicamente isolado

Para compartilhar um cofre logicamente isolado,

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, selecione Pilhas.
3. Abaixo das descrições dos cofres, haverá duas listas: Cofres de propriedade dessa conta e Cofres compartilhados com essa conta. Selecione a lista desejada para ver os cofres.
4. Em Nome do cofre, selecione o nome do cofre logicamente isolado para abrir a página de detalhes.
5. O painel de compartilhamento de contas mostra com quais contas o cofre está sendo compartilhado.
6. Para começar a compartilhar com outra conta ou editar as contas que já estão sendo compartilhadas, selecione Gerenciar compartilhamento.

AWS RAM o console é aberto quando a opção Gerenciar compartilhamento é selecionada. Para ver as etapas para compartilhar um recurso usando a AWS RAM, consulte Criação de um compartilhamento de recursos na AWS RAM.

Verifique se você tem as permissões apropriadas. Backup Administrator IAM Policy [AWSBackupFullAccess] e Backup Operator IAM Policy [AWSBackupOperatorAccess] contêm a permissão necessária para visualizar contas compartilhadas; no entanto, a função que você usa para compartilhar precisa de permissões de gravação do Resource Access Manager para compartilhar a conta da RAM, como`ram:CreateResourceShare`.

A conta convidada a aceitar um convite para receber um compartilhamento tem 12 horas para aceitar o convite. Consulte Aceitar e rejeitar convites de compartilhamento de recursos no Guia do usuário do AWS RAM.

Se as etapas de compartilhamento forem concluídas e aceitas, a página de resumo do cofre será exibida em Compartilhamento de conta = “Compartilhado - veja a tabela de compartilhamento de conta abaixo”.

Restaurar um backup de um cofre logicamente isolado usando o console

Você pode restaurar um backup armazenado em um cofre logicamente isolado a partir da conta proprietária do cofre ou de qualquer conta com a qual o cofre seja compartilhado.

Consulte Restaurar um backup para obter informações sobre como restaurar um ponto de recuperação.

Excluir um cofre logicamente isolado usando o console

> **Important**
>
> Quando o serviço se tornar disponível ao público em geral, os dados e as configurações fornecidos durante a pré-visualização não estarão mais disponíveis. AWS recomenda usar dados de teste em vez de dados de produção com a visualização prévia.

Consulte excluir um cofre de backup para excluir um cofre. Os cofres não poderão ser excluídos se ainda contiverem backups (pontos de recuperação). Certifique-se de que o cofre não tenha nenhum backup antes de iniciar uma operação de exclusão.

Cofres logicamente isolados por meio de CLI/API

Você pode usar AWS CLI para realizar operações de forma programática em cofres logicamente isolados. Cada CLI é específica para o AWS serviço em que se origina. Os comandos relacionados ao compartilhamento são prefixados com `aws ram`. Todos os outros comandos devem ser prefixados com `aws backup`.

Criar

O exemplo de comando `CreateLogicallyAirGappedBackupVault` da CLI pode ser modificado para criar um cofre de backup logicamente isolado:

```
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
```

Visualizar os detalhes

O exemplo de comando `DescribeBackupVault` da CLI a seguir pode ser modificado para obter os detalhes sobre um cofre:

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

Compartilhar

> **Note**
>
> Somente contas com permissões suficientes do IAM podem compartilhar e gerenciar o compartilhamento de contas.

É possível pode compartilhar um cofre logicamente isolado por meio do AWS Resource Access Manager (RAM), um serviço que ajuda os usuários a compartilhar recursos.

AWS RAM usa o comando CLI. `create-resource-share` O acesso a esse comando só está disponível para contas de administrador com permissões suficientes. Consulte Criar um compartilhamento de recursos no AWS RAM para ver as etapas da CLI.

As etapas de 1 a 4 são conduzidas com a conta proprietária do cofre logicamente isolado. As etapas 5 a 8 são conduzidas com a conta com a qual o cofre logicamente isolado será compartilhado.

1. Faça login na conta proprietária OU solicite que um usuário em sua organização com credenciais suficientes para acessar a conta de origem conclua essas etapas.
   - Se um compartilhamento de recursos foi criado anteriormente e você deseja adicionar um recurso adicional a ele, use `associate-resource-share` da CLI em vez disso com o ARN do novo cofre.
2. Obtenha as credenciais de uma função com permissões suficientes para compartilhar via RAM. Insira-as na CLI.
   - A permissão `ram:CreateResourceShare` é necessária para esse procedimento. A política AWSResourceAccessManagerFullAccesscontém todas as permissões relacionadas à RAM.

3. Use create-resource-share.

   a. Inclua o ARN do cofre logicamente isolado.

   b. Exemplo 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
```

   Resultado do exemplo:

```
{
   "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 o ARN do compartilhamento de recursos no resultado (que é necessário para as etapas subsequentes). Forneça o ARN ao operador da conta que você está convidando para receber o compartilhamento.

5. Obter o ARN do compartilhamento de recursos

   a. Se você não executou as etapas de 1 a 4, obtenha-as resourceShareArn de quem as executou.

   b. Exemplo: `arn:aws:ram:us-east-1:123456789012:resource-share/12345678-abcd-09876543`

6. Na CLI, assuma as credenciais da conta destinatária.

7. Receba um convite para compartilhar recursos com `get-resource-share-invitations`. Para obter mais informações, consulte Aceitar e rejeitar convites no Guia do usuário do AWS RAM .
8. Aceite o convite na conta de destino (recuperação).
    - Use `accept-resource-share-invitation` (também é possível usar `reject-resource-share-invitation`).

Lista

O comando `ListBackupVaults` da CLI pode ser modificado para listar todos os cofres de propriedade e presentes na conta:

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

Para listar apenas os cofres logicamente isolados, adicione o parâmetro

```

--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

Para listar cofres compartilhados com a conta, use

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

Copiar

Um cofre logicamente isolado só pode ser o destino de um trabalho de cópia de um backup, não o destino de um trabalho inicial de backup. Use `StartCopyJob` para copiar um backup existente em um cofre de backup para um cofre logicamente isolado.

A função que está sendo usada para criar o trabalho de cópia para o cofre logicamente isolado deve conter a permissão `kms:CreateGrant`.

Exemplo de entrada da 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

Depois que um backup for compartilhado de um cofre logicamente isolado na sua conta, você poderá usar `StartRestoreJob` para restaurar o backup. Exemplo de entrada da 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

O exemplo de comando `DeleteBackupVault` da CLI pode ser usado para excluir um cofre. Um cofre só poderá ser excluído se não houver backups (pontos de recuperação) dentro dele.

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

Outras opções programáticas disponíveis incluem:

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

Criar um cofre de backup

Você deve criar pelo menos um cofre antes de criar um plano de backup ou iniciar uma tarefa de backup.

Quando você usa o AWS Backup console pela primeira vez em um Região da AWS, o console cria automaticamente um cofre padrão.

No entanto, se você usar AWS Backup por meio do AWS CLI AWS SDK ou AWS CloudFormation, um cofre padrão não será criado. Você deverá criar seu próprio cofre.

Permissões obrigatórias

Você deve ter as seguintes permissões para criar um cofre de backup usando 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": "*"
    }
  ]
}
```

Criar um cofre de backup (console)

Para step-by-step obter instruções sobre como criar um cofre de backup usando o AWS Backup console, consulte Etapa 3: criar um cofre de backup o guia de introdução.

Criar um cofre de backup (programaticamente)

O AWS Command Line Interface comando a seguir cria um cofre de backup:

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

Você também pode especificar as seguintes configurações para um cofre de backup.

Nome do cofre de backup

Os nomes dos cofres de backup fazem distinção de maiúsculas de minúsculas. Eles devem conter de 2 a 50 caracteres alfanuméricos, hífens ou sublinhados.

AWS KMS chave de criptografia

A chave de AWS KMS criptografia protege seus backups nesse cofre de backup. Por padrão, o AWS Backup cria uma chave do KMS com o alias `aws/backup` para você. Você pode escolher essa chave ou escolher qualquer outra chave em sua conta (é possível usar chaves do KMS entre contas via CLI).

Você pode criar uma chave de criptografia seguindo o procedimento de criação de chaves no Guia do desenvolvedor do AWS Key Management Service .

Depois de criar um cofre de backup e definir a chave de AWS KMS criptografia, você não poderá mais editar a chave desse cofre de backup.

A chave de criptografia especificada em um AWS Backup cofre se aplica aos backups de determinados tipos de recursos. Para obter mais informações sobre a criptografia de backup, consulte Criptografia para backups em AWS Backup na seção Segurança. Os backups de todos os outros tipos de recurso são feitos com a chave usada para criptografar o recurso de origem.

Tags do cofre de backup

Essas tags são associadas ao cofre de backup para ajudar você a organizar e acompanhar cofres de backup.

Definir políticas de acesso em cofres de backup

Com AWS Backup, você pode atribuir políticas aos cofres de backup e aos recursos que eles contêm. A atribuição de políticas permite que você faça várias coisas, como conceder acesso aos usuários para criar planos de backup e backups sob demanda, mas limite a capacidade delas de excluir pontos de recuperação depois que eles tiverem sido criados.

Para obter informações sobre como usar políticas para conceder ou restringir o acesso a recursos, consulte Políticas baseadas em identidade e políticas baseadas em recursos no Guia do usuário do IAM. Também é possível controlar o acesso usando tags.

Você pode usar os exemplos de políticas a seguir como guia para limitar o acesso aos recursos ao trabalhar com AWS Backup cofres. Ao contrário de outras políticas baseadas em IAM, as políticas de AWS Backup acesso não oferecem suporte a um curinga na chave. `Action`

Para obter uma lista de nomes de recursos da Amazon (ARNs) que podem ser usados para identificar pontos de recuperação de diferentes tipos de recursos, consulte AWS Backup ARNs de recursos para ARNs de pontos de recuperação específicos dos recursos.

As políticas de acesso ao Vault controlam apenas o acesso do usuário às AWS Backup APIs. Alguns tipos de backup, como snapshots do Amazon Elastic Block Store (Amazon EBS) e do Amazon Relational Database Service (Amazon RDS), também podem ser acessadas usando as APIs desses serviços. Você pode criar políticas de acesso separadas no IAM, que controlam o acesso a essas APIs, para controlar totalmente o acesso a esses tipos de backup.

Independentemente da política de acesso do AWS Backup cofre, o acesso entre contas para qualquer ação que não seja `backup:CopyIntoBackupVault` será rejeitado, ou seja, AWS Backup rejeitará qualquer outra solicitação de uma conta diferente da conta do recurso que está sendo referenciado.

Tópicos

- Negar acesso a um tipo de recurso em um cofre de backup
- Negar acesso a um cofre de backup
- Negar acesso para excluir pontos de recuperação em um cofre de backup

Negar acesso a um tipo de recurso em um cofre de backup

Esta política nega acesso às operações de API especificadas para todos os snapshots do EBS em um cofre de backup.

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

Negar acesso a um cofre de backup

Esta política nega acesso às operações de API especificadas que visam um cofre de backup.

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

Negar acesso para excluir pontos de recuperação em um cofre de backup

O acesso aos cofres e a capacidade de excluir pontos de recuperação armazenados neles são determinados pelo acesso que você conceder aos seus usuários.

Siga estas etapas para criar uma política de acesso baseada em recursos em um cofre de backup que impede a exclusão de todos os backups no cofre.

Como criar uma política de acesso baseada em recursos em um cofre de backup

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação no lado esquerdo, selecione Cofres de backup.
3. Selecione um cofre de backup na lista.
4. Na seção de Política de acesso, cole o seguinte exemplo de JSON. Esta política impede que qualquer pessoa que não seja a principal exclua um ponto de recuperação no cofre de backup de destino.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:userId": [
                        "AAAAAAAAAAAAAAAAAAAAA:",
                        "BBBBBBBBBBBBBBBBBBBBB",
                        "112233445566"
                    ]
                }
            }
        }
    ]
}
```

Para permitir listar identidades do IAM usando seu ARN, use a chave de condição global `aws:PrincipalArn` no exemplo a seguir.

```
{
    "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 obter informações sobre como obter um ID exclusivo para uma entidade do IAM, consulte Obter o identificador exclusivo no Guia do usuário do IAM.

Se quiser que isso seja limitado a tipos de recursos específicos, em vez de `"Resource": "*"`, você poderá incluir explicitamente os tipos de ponto de recuperação a serem negados. Por exemplo, para snapshots do Amazon EBS, altere o tipo de recurso para o seguinte:

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

5. Escolha Anexar política.

AWS Backup Fechadura do cofre

> **Note**
>
> AWS Backup O Vault Lock foi avaliado pela Cohasset Associates para uso em ambientes sujeitos às regulamentações SEC 17a-4, CFTC e FINRA. Para obter mais informações sobre como o AWS Backup Vault Lock se relaciona com esses regulamentos, consulte a Avaliação de conformidade da Cohasset Associates.

AWS Backup O Vault Lock é um recurso opcional de um cofre de backup, que pode ser útil para oferecer segurança e controle adicionais sobre seus cofres de backup. Quando um bloqueio está ativo no modo de conformidade e o tempo de carência termina, a configuração do cofre não poderá ser alterada ou excluída por um cliente, proprietário da conta/dados ou pela AWS. Cada cofre pode ter um bloqueio de cofre em vigor.

AWS Backup garante que seus backups estejam disponíveis para você até que atinjam a expiração dos períodos de retenção. Se algum usuário (incluindo o usuário raiz) tentar excluir um backup ou alterar as propriedades do ciclo de vida em um cofre bloqueado, AWS Backup negará a operação.

- Os cofres bloqueados no modo de governança podem ter o bloqueio removido por usuários com permissões suficientes do IAM.
- Os cofres bloqueados no modo de conformidade não podem ser excluídos depois que o período de reflexão (“período de carência”) expirar. Durante o período de carência, você ainda pode remover o bloqueio do cofre e alterar a configuração do bloqueio.

Modos de bloqueio do cofre

Ao criar um bloqueio de cofre, você pode escolher entre dois modos: modo de governança ou modo de conformidade. O modo de governança tem como objetivo permitir que um cofre seja gerenciado somente por usuários com privilégios suficientes do IAM. O modo de governança ajuda a organização a atender aos requisitos de governança, garantindo que somente a equipe designada

possa fazer alterações em um cofre de backup. O modo de conformidade é destinado a cofres de backup nos quais se espera que o cofre (e, por extensão, seu conteúdo) nunca seja excluído ou alterado até que o período de retenção de dados seja concluído. Quando um cofre no modo de conformidade é bloqueado, ele é imutável, o que significa que o bloqueio não pode ser removido.

Um cofre bloqueado no modo de governança pode ser gerenciado ou excluído por usuários que tenham as permissões apropriadas do IAM.

Um bloqueio de cofre no modo de conformidade não pode ser alterado ou excluído por nenhum usuário ou pela AWS. Um bloqueio de cofre no modo de conformidade tem um período de carência que você define antes de ser bloqueado e se tornar imutável.

Benefícios do Vault Lock

AWS Backup O Vault Lock oferece vários benefícios, incluindo:

- Configuração WORM (write once, read-many) para todos os backups que você armazena e cria em um cofre de backup.
- Uma camada adicional de defesa que protege os backups (pontos de recuperação) em seus cofres de backup contra exclusões inadvertidas ou mal-intencionadas.
- Aplicação de períodos de retenção, que evitam exclusões antecipadas por usuários privilegiados (incluindo o usuário Conta da AWS raiz) e atendem às políticas e procedimentos de proteção de dados da sua organização.

Bloquear um cofre de backup usando o console

Você pode adicionar uma trava de cofre ao seu AWS Backup cofre usando o console de Backup.

Como adicionar um bloqueio de cofre ao seu cofre de backup:

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Cofres de backup. Clique no link aninhado em Cofres de backup chamado Bloqueios de cofre.
3. Em Como funcionam os bloqueios do cofre ou Bloqueios de cofre, clique em + Criar bloqueio de cofre.
4. No painel Detalhes do bloqueio de cofre, escolha em qual cofre você deseja aplicar o bloqueio.

5. Em Modo de bloqueio de cofre, escolha em qual modo você deseja que seu cofre seja bloqueado. Para obter mais informações sobre como escolher seus modos, consulte Modos de bloqueio de cofre anteriormente nesta página.
6. Para o período de retenção, escolha os períodos mínimo e máximo de retenção (os períodos de retenção são opcionais). Haverá falha nos novos trabalhos de backup e cópia criados no cofre se não estiverem em conformidade com os períodos de retenção que você definiu. Esses períodos não se aplicarão aos pontos de recuperação que já estiverem no cofre.
7. Se você escolher o modo de conformidade, uma seção chamada Data de início do bloqueio de cofre será exibida. Se você escolher o modo de governança, isso não será exibido e essa etapa poderá ser ignorada.

   No modo de conformidade, um bloqueio de cofre tem um período de reflexão desde a criação do bloqueio até que o cofre e seu bloqueio se tornem imutáveis e inalteráveis. Você escolhe a duração desse período (chamado de período de carência), embora deva ser de pelo menos três dias (72 horas).

   > **Important**
   >
   > Depois que o período de carência expirar, o cofre e seu bloqueio serão imutáveis. Ele não pode ser alterado ou excluído por nenhum usuário ou pela AWS.

8. Quando estiver satisfeito com as opções de configuração, clique em Criar bloqueio de cofre.
9. Para confirmar que você deseja criar esse bloqueio no modo escolhido, digite `confirm` na caixa de texto e marque a caixa confirmando que a configuração está conforme pretendido.

Se as etapas tiverem sido concluídas com êxito, um banner “Êxito” será exibido na parte superior do console.

Bloquear um cofre de backup de forma programática

Para configurar o AWS Backup Vault Lock, use a API`PutBackupVaultLockConfiguration`. Os parâmetros a serem incluídos dependerão do modo de bloqueio do cofre que você pretende usar. Se você deseja criar um bloqueio de cofre no modo de governança, não inclua `ChangeableForDays`. Se esse parâmetro for incluído, o bloqueio do cofre será criado no modo de conformidade.

Aqui está um exemplo de CLI da criação de um bloqueio de cofre no modo de conformidade:

```
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
```

Aqui está um exemplo de CLI da criação de um bloqueio de cofre no modo de governança:

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

É possível configurar quatro opções.

1. **`BackupVaultName`**

   O nome do cofre a ser bloqueado.

2. **`ChangeableForDays`** (inclua somente para o modo de conformidade)

   Esse parâmetro instrui AWS Backup a criar o bloqueio do cofre no modo de conformidade. Omita esse parâmetro se você pretende criar o bloqueio no modo de governança.

   Esse valor é expresso em dias. Deve ser um número não menor que 3 e não maior que 36.500. Caso contrário, será retornado um erro.

   Desde a criação desse bloqueio de cofre até a expiração da data especificada, o bloqueio do cofre poderá ser removido do cofre usando `DeleteBackupVaultLockConfiguration`. Como alternativa, durante esse período, você poderá alterar a configuração usando `PutBackupVaultLockConfiguration`.

   Na data especificada e determinada por esse parâmetro, o cofre de backup será imutável e não poderá ser alterado ou excluído.

3. **`MaxRetentionDays`** (opcional)

   Esse é um valor numérico expresso em dias. Esse é o período máximo de retenção que o cofre retém seus pontos de recuperação.

   O período máximo de retenção que você escolher deve estar alinhado com as políticas de retenção de dados da sua organização. Se a sua organização instruir que os dados sejam retidos por um período, esse valor poderá ser definido para esse período (em dias). Por exemplo, pode

ser necessário manter dados financeiros ou bancários por sete anos (aproximadamente 2.557 dias, dependendo dos anos bissextos).

Se não for especificado, o AWS Backup Vault Lock não aplicará um período máximo de retenção. Se especificado, haverá falha nos trabalhos de backup e cópia para esse cofre com períodos de retenção do ciclo de vida superiores ao período máximo de retenção. Os pontos de recuperação já salvos no cofre antes da criação do bloqueio de cofre não serão afetados. O período máximo de retenção mais longo que você pode especificar é de 36.500 dias (aproximadamente 100 anos).

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

   Esse é um valor numérico expresso em dias. Esse é o período mínimo de retenção que o cofre retém seus pontos de recuperação. Essa configuração deve ser definida de acordo com a quantidade de tempo que sua organização deve manter os dados. Por exemplo, se os regulamentos ou leis exigirem que os dados sejam retidos por pelo menos sete anos, o valor em dias seria de aproximadamente 2.557, dependendo dos anos bissextos.

   Se não for especificado, o AWS Backup Vault Lock não aplicará um período mínimo de retenção. Se especificado, haverá falha nos trabalhos de backup e cópia para esse cofre com períodos de retenção do ciclo de vida inferiores ao período mínimo de retenção. Os pontos de recuperação já salvos no cofre antes do AWS Backup Vault Lock não são afetados. O período mínimo de retenção mais curto que você pode especificar é de um dia.

Revise a configuração do Vault Lock em um AWS Backup cofre de backup

Você pode revisar os detalhes do AWS Backup Vault Lock em um cofre a qualquer momento por meio de chamadas `DescribeBackupVault` ou APIs. `ListBackupVaults`

Para determinar se você aplicou um bloqueio de cofre a um cofre de backup, chame `DescribeBackupVault` e verifique a propriedade `Locked`. Se`"Locked": true`, como no exemplo a seguir, você aplicou o AWS Backup Vault Lock ao seu cofre de backup.

```
{
    "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"
}
```

A saída anterior confirma as seguintes opções:

1. `Locked`é um booleano que indica se você aplicou o AWS Backup Vault Lock a esse cofre de backup. `True`significa que o AWS Backup Vault Lock faz com que as operações de exclusão ou atualização dos pontos de recuperação armazenados no cofre falhem (independentemente de você ainda estar no período de carência de reflexão).
2. `LockDate` é a data e a hora em UTC em que seu período de carência de reflexão termina. Após esse período, você não poderá excluir ou alterar seu bloqueio neste cofre. Use qualquer conversor de horário disponível publicamente para converter essa string em sua hora local.

Se `"Locked":false`, como no exemplo a seguir, você não tiver aplicado um bloqueio de cofre (ou se um anterior tiver sido excluído).

```
{
    "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
}
```

Remoção do bloqueio do cofre durante o período de carência (modo de conformidade)

Para excluir o bloqueio do cofre durante o período de carência (o tempo após o bloqueio do cofre, mas antes do seu`LockDate`) usando o console, AWS Backup

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, em Minha conta, clique em Cofres de backup e, em seguida, clique em Backup Vault Lock.
3. Clique no bloqueio do cofre que você deseja remover e, em seguida, clique em Gerenciar bloqueio de cofre.
4. Clique em Excluir cofre.
5. Uma caixa de aviso será exibida solicitando que você confirme sua intenção de excluir o bloqueio do cofre. Digite `confirm` na caixa de texto e clique em confirmar.

Depois que todas as etapas forem concluídas com êxito, um banner de Êxito será exibido na parte superior da tela do console.

Para excluir o bloqueio do cofre durante o período de carência usando um comando da CLI, use `DeleteBackupVaultLockConfiguration` como este exemplo de CLI:

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

Conta da AWS fechamento com um cofre trancado

Quando você fecha um Conta da AWS que contém um cofre de backup AWS e AWS Backup suspende sua conta por 90 dias com seus backups intactos. Se você não reabrir sua conta durante esses 90 dias, AWS excluirá o conteúdo do seu cofre de backup, mesmo se o AWS Backup Vault Lock estiver em vigor.

Considerações adicionais sobre segurança

AWS Backup O Vault Lock adiciona uma camada adicional de segurança à sua defesa de proteção de dados em profundidade. É possível combinar o bloqueio do cofre com esses outros recursos de segurança:

- Criptografia para seus pontos de recuperação
- AWS Backup políticas de acesso ao cofre e ao ponto de recuperação, que permitem conceder ou negar permissões no nível do cofre,

- AWS Backup melhores práticas de segurança, incluindo sua biblioteca de políticas gerenciadas pelo cliente que permitem que você conceda ou negue permissões de backup e restauração por meio de um serviço AWS compatível, e
- AWS Backup Audit Manager, que permite automatizar as verificações de conformidade de seus backups em relação a uma lista de controles definidos por você.

  Você pode realizar Criação de estruturas usando a API AWS Backup para o controle Os backups são protegidos pelo AWS Backup Vault Lock com o AWS Backup Audit Manager para ajudar a garantir que os recursos pretendidos sejam protegidos com um bloqueio de cofre.
- Mecanismos que tornam os recursos inativos podem afetar a capacidade de restaurá-los. Embora ainda não possam ser excluídos em um cofre trancado, eles podem estar em um estado diferente de ativos. Por exemplo, a configuração do Amazon Elastic Compute Cloud que permite que você desabilite uma AMI pode bloquear temporariamente a capacidade de restaurar backups de instâncias do EC2. Isso afeta todos os pontos de recuperação do EC2, até mesmo os backups afetados por um bloqueio do cofre ou por uma retenção legal.

  Se um backup do EC2 estiver desativado, você poderá reativar uma AMI desativada. Depois de reativado, ele está qualificado para ser restaurado. Para bloquear o recurso de desativação da AMI, você pode usar políticas do IAM para não permitir`ec2:DisableImage`.

> **Note**
>
> AWS Backup O Vault Lock não é o mesmo recurso do Amazon S3 Glacier Vault Lock, que é compatível somente com o S3 Glacier.

Excluir um cofre de backup

Para se proteger contra a exclusão em massa acidental ou maliciosa, você pode excluir um cofre de backup no AWS Backup somente depois de excluir (ou os ciclos de vida do seu plano de backup) todos os pontos de recuperação em seu cofre de backup. Para excluir seus pontos de recuperação manualmente, consulte Limpar recursos.

Ao excluir um cofre de backup, atualize seus planos de backup a serem direcionados a novos cofres de backup. Um plano de backup que é direcionado para um cofre de backup excluído fará com que a criação de backup falhe.

> **Note**
>
> Você não pode excluir dois cofres de backup: o cofre de backup AWS Backup padrão e o cofre de backup automático do Amazon EFS.

Para excluir um cofre de backup usando o console AWS Backup

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Cofres de Backup.
3. Escolha o nome do cofre de backup para abrir sua página de detalhes.
4. Escolha e exclua todos os backups associados ao cofre de backup.
5. Escolha Excluir cofre. Quando a confirmação for solicitada, insira o nome do cofre e escolha Excluir cofre de Backup.

Trabalhar com backups

Um backup, ou ponto de recuperação, representa o conteúdo de um recurso, como um volume do Amazon Elastic Block Store (Amazon EBS) ou uma tabela do Amazon DynamoDB, em um determinado momento. Ponto de recuperação é um termo que geralmente se refere aos diferentes backups em AWS serviços, como snapshots do Amazon EBS e backups do DynamoDB. Os termos ponto de recuperação e backup são usados de forma intercambiável.

AWS Backup salva pontos de recuperação em cofres de backup, que você pode organizar de acordo com as necessidades da sua empresa. Por exemplo, você pode salvar um conjunto de recursos que contenham informações financeiras para o ano fiscal de 2020. Quando precisar recuperar um recurso, você pode usar o AWS Backup console ou o AWS Command Line Interface (AWS CLI) para encontrar e recuperar o recurso de que precisa.

Cada ponto de recuperação tem um ID exclusivo. O ID exclusivo estará no final do Nome do recurso da Amazon (ARN) do ponto de recuperação. Para exemplos de ARNs de pontos de recuperação e IDs exclusivos, consulte a tabela em Recursos e operações.

> **Important**
>
> Para evitar cobranças adicionais, configure sua política de retenção com uma duração de armazenamento quente de pelo menos uma semana. Para ter mais informações, consulte Medição, custos e cobrança.

As seções a seguir fornecem uma visão geral das tarefas básicas de gerenciamento de backup no AWS Backup.

Tópicos

Criar um backup

Com AWS Backup, você pode criar backups automaticamente usando planos de backup ou manualmente iniciando um backup sob demanda.

Criar backups automáticos

Quando os backups são criados automaticamente pelo planos de backup, eles são configurados com as configurações de ciclo de vida que estão definidas no plano de backup. Eles são organizados no cofre de backup que é especificado no plano de backup. Também são atribuídos às tags listadas no plano de backup. Para obter mais informações sobre planos de backups, consulte Gerenciar backups usando planos de backup.

Criar backups sob demanda

Quando você cria um backup sob demanda, você pode definir essas configurações para o backup que está sendo criado. Quando um backup é criado automaticamente ou manualmente, um trabalho de backup é iniciado. Para saber como criar um backup sob demanda, consulte Criando um backup sob demanda usando AWS Backup.

Nota: um backup sob demanda cria um trabalho de backup; a transição do trabalho de backup ocorrerá em um estado de `Running` dentro de uma hora (ou quando especificado). É possível optar um backup sob demanda se você quiser criar um backup em um horário diferente do horário programado definido em um plano de backup. Um backup sob demanda pode ser usado, por exemplo, para testar o backup e a funcionalidade a qualquer momento.

Os backups sob demanda não podem ser usados com point-in-time restauração (PITR), pois um backup sob demanda preserva os recursos no estado em que estão quando o backup é feito, enquanto o PITR usa backups contínuos que registram as alterações durante um período de tempo.

Status do trabalho de backup

Cada trabalho de backup tem um ID exclusivo. Por exemplo, `D48D8717-0C9D-72DF-1F56-14E703BF2345`.

Você pode visualizar o status de um trabalho de backup na página Trabalhos do console do AWS Backup . Os status da tarefa de backup incluem `CREATEDPENDING`,`RUNNING`,`ABORTING`,`ABORTED`,`COMPLETED`,`FAILED`,`EXPIRED`, e. `PARTIAL`

Como funcionam os backups incrementais

Muitos recursos oferecem suporte ao backup incremental com AWS Backup. Uma lista completa está disponível na seção de backup incremental da tabela Disponibilidade de recursos por recurso.

Embora cada backup após o primeiro seja incremental (ou seja, ele captura apenas as alterações do backup anterior), todos os backups feitos com AWS Backup retêm os dados de referência necessários para permitir uma restauração completa. Isso é verdade mesmo que o backup original (completo) tenha chegado ao fim de seu ciclo de vida e tenha sido excluído.

Por exemplo, se seu backup do dia 1 (completo) fosse excluído devido a uma política de ciclo de vida de 3 dias, você ainda poderia realizar uma restauração completa com os backups dos dias 2 e 3. O AWS Backup mantém os dados de referência necessários do dia 1 para fazer isso.

Acesso aos recursos de origem

AWS Backup precisa acessar seus recursos de origem para fazer backup deles. Por exemplo: .

- Para fazer backup de uma instância do Amazon EC2, a instância pode estar no estado `stopped` ou `running` , mas não no estado `terminated`. Isso ocorre porque uma `stopped` instância `running` or pode se comunicar com AWS Backup, mas uma `terminated` instância não.
- Para fazer backup de uma máquina virtual, o hipervisor deve ter o status `ONLINE` do gateway de backup. Para obter mais informações, consulte Noções básicas do status do hipervisor.
- Para fazer backup de um banco de dados do Amazon RDS, do Amazon Aurora ou de um cluster do Amazon DocumentDB, esses recursos devem ter o status `AVAILABLE`.
- Para fazer backup de um Amazon Elastic File System (Amazon EFS), ele deve ter o status `AVAILABLE`.
- Para fazer backup de um sistema de arquivos do Amazon FSx, ele deve ter o status `AVAILABLE`. Se o status for `UPDATING`, a solicitação de backup será colocada na fila até que o sistema de arquivos se torne `AVAILABLE`.

  O FSx para ONTAP não é compatível com o backup de determinados tipos de volume, incluindo volumes de DP (proteção de dados), volumes de LS (compartilhamento de carga), volumes completos ou volumes em sistemas de arquivos que estão cheios. Para ter mais informações, consulte FSx para ONTAP – trabalhar com backups.

AWS Backup mantém os backups criados anteriormente de acordo com sua política de ciclo de vida, independentemente da integridade do seu recurso de origem.

Tópicos

Criando um backup sob demanda usando AWS Backup

No AWS Backup console, a página Recursos protegidos lista os recursos que foram copiados pelo AWS Backup menos uma vez. Se você estiver usando AWS Backup pela primeira vez, não há recursos (como volumes do Amazon EBS ou bancos de dados do Amazon RDS) listados nesta página. Isso se aplica mesmo que esse recurso tenha sido atribuído a um plano de backup que não tenha executado um trabalho de backup programado pelo menos uma vez.

Observação: um backup sob demanda começa a fazer backup do seu recurso imediatamente. É possível optar um backup sob demanda se você quiser criar um backup em um horário diferente do horário programado definido em um plano de backup. Um backup sob demanda pode ser usado, por exemplo, para testar o backup e a funcionalidade a qualquer momento.

Os backups sob demanda não podem ser usados com point-in-time restauração (PITR), pois um backup sob demanda preserva os recursos no estado em que estão quando o backup é feito, enquanto o PITR usa backups contínuos que registram as alterações durante um período de tempo.

Considerações

- Se a função AWS Backup padrão não estiver presente na sua conta, uma será criada para você com as permissões corretas.
- Quando os backups expirarem e forem marcados para exclusão como parte de sua política de ciclo de vida, o AWS Backup excluirá os backups em um ponto escolhido aleatoriamente nas 8 horas seguintes. Essa janela ajuda a garantir um desempenho consistente.
- Para recursos do Amazon EC2, copia AWS Backup automaticamente as tags existentes de grupos e recursos individuais, além das tags que você adicionar nesta etapa.
- AWS Backup usa backups do EC2 sem “reinicialização” como comportamento padrão. AWS Backup atualmente oferece suporte a recursos executados no Amazon EC2, e certos tipos de instância não são suportados. Para ter mais informações, consulte Criar backups do VSS do Windows.

Como criar um backup sob demanda

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel, escolha Criar um backup sob demanda. Ou, no painel de navegação, escolha Recursos protegidos e Criar backup sob demanda.
3. Na página Tipo de recurso, escolha o tipo de recurso do qual você deseja fazer backup. Por exemplo, escolha o DynamoDB para tabelas do Amazon DynamoDB.
4. Escolha o nome ou ID do recurso a ser protegido. Por exemplo, escolha o nome da tabela do DynamoDB para o Amazon DynamoDB.
5. Certifique-se de que a opção Criar backup agora esteja selecionada.
6. Se o tipo de recurso suportar a transição para o armazenamento a frio, o armazenamento a frio estará presente. Para obter mais informações, consulte a coluna Ciclo de vida até armazenamento refrigerado na tabela Disponibilidade de recursos por recurso.

   Para especificar quando esse backup vai para o armazenamento frio, escolha Mover backups do armazenamento quente para o armazenamento frio e, em seguida, especifique o tempo no armazenamento a quente.
7. Em Período total de retenção, especifique o número de dias. Se você especificou o tempo em armazenamento refrigerado, o período de retenção é dividido entre armazenamento quente e frio.

8. Escolha um Cofre de backup existente ou crie um. Ao escolher Criar cofre de backup, uma nova página será aberta para criar um cofre e você será redirecionado para a página Criar backup sob demanda ao concluir.
9. Para a função do IAM, escolha a função padrão ou uma função que você criou.
10. Para atribuir uma tag ao seu backup sob demanda, expanda Tags adicionadas aos pontos de recuperação, escolha Adicionar nova tag e insira a chave e o valor da tag.
11. Se o tipo de recurso for EC2, as configurações avançadas de backup estarão presentes. Para tirar instantâneos consistentes com aplicativos usando o Windows Volume Shadow Copy Service (VSS), escolha Windows VSS.
12. Escolha Criar backup sob demanda. Isso abre a página Trabalhos, onde você pode ver uma lista de trabalhos e ver o status do trabalho.

Backups e point-in-time restauração contínuos (PITR)

Tópicos

Para alguns recursos, AWS Backup oferece suporte a backups e point-in-time recuperação contínuos (PITR), além de backups instantâneos.

Com backups contínuos, você pode restaurar seu recurso AWS Backup suportado rebobinando-o para um horário específico de sua escolha, com precisão de 1 segundo (retrocesso máximo de 35 dias). O backup contínuo funciona criando primeiramente um backup completo do seu recurso e, em seguida, fazendo backup constante dos logs de transações do recurso. A restauração da PITR funciona acessando seu backup completo e reproduzindo o registro de transações até o momento em que você solicita AWS Backup a recuperação.

Como alternativa, os backups de snapshot podem ser feitos a cada hora. Os backups de snapshot podem ser armazenados por um máximo de até 100 anos. Os snapshots podem ser copiados em backups completos ou incrementais.

Como os backups contínuos e de snapshot oferecem vantagens diferentes, recomendamos que você proteja seus recursos com regras de backup contínuo e de snapshot.

Observação: um backup sob demanda começa a fazer backup do seu recurso imediatamente. É possível optar um backup sob demanda se você quiser criar um backup em um horário diferente do horário programado definido em um plano de backup. Um backup sob demanda pode ser usado, por exemplo, para testar o backup e a funcionalidade a qualquer momento.

Os backups sob demanda não podem ser usados com point-in-time restauração (PITR), pois um backup sob demanda preserva os recursos no estado em que estão quando o backup é feito, enquanto o PITR usa backups contínuos que registram as alterações durante um período de tempo.

Você pode optar por backups contínuos dos recursos compatíveis ao criar um plano de backup AWS Backup usando o AWS Backup console ou a API.

Como habilitar os backups contínuos usando o console

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Planos de backup e, depois, escolha Criar plano.
3. Em Regras de backup, escolha Adicionar regra de backup.
4. Na seção Configuração da regra de backup, selecione Habilitar backups contínuos para recursos compatíveis.

Serviços compatíveis para backup contínuo/restauração pontual (PITR)

AWS Backup oferece suporte a backups e point-in-time recuperação contínuos para os seguintes serviços e aplicativos:

Amazon S3

Para ativar a PITR para backups do S3, os backups contínuos precisam fazer parte do plano de backup.

Embora esse backup original do bucket de origem possa ter a PITR ativa, as cópias de destino entre regiões ou entre contas não terão a PITR, e a restauração a partir dessas cópias será restaurada no

momento em que foram criadas (as cópias serão cópias de snapshot) em vez de serem restauradas para um ponto no tempo específico.

RDS

Programações de backup: Quando um AWS Backup plano cria tanto instantâneos do Amazon RDS quanto backups contínuos, AWS Backup programará de forma inteligente suas janelas de backup para coordenar com a janela de manutenção do Amazon RDS para evitar conflitos. Para evitar ainda mais conflitos, a configuração manual da janela de backup automático do Amazon RDS não está disponível. O RDS tira snapshots uma vez por dia, independentemente de o plano de backup ter uma frequência para backups de snapshot diferente de uma vez por dia.

Configurações: Depois de aplicar uma regra de backup AWS Backup contínuo a uma instância do Amazon RDS, você não pode criar ou modificar configurações de backup contínuo para essa instância no Amazon RDS; as modificações devem ser feitas por meio do AWS Backup console ou da CLI AWS Backup .

Controle de transição do backup contínuo de uma instância do Amazon RDS de volta para o Amazon RDS:

Console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Planos de backup.
3. Exclua todos os planos de backup do Amazon RDS com backup contínuo que protegem esse recurso.
4. Escolha Cofres de backup. Exclua o ponto de recuperação de backup contínuo do seu cofre de backup. Ou aguarde o término do período de retenção, fazendo com que o ponto de recuperação AWS Backup seja excluído automaticamente.

Depois de concluir essas etapas, AWS Backup fará a transição do controle de backup contínuo do seu recurso de volta para o Amazon RDS.

AWS CLI

Chame a operação da API `DisassociateRecoveryPoint`.

Para saber mais, consulte DisassociateRecoveryPoint.

Permissões do IAM necessárias para backups contínuos do Amazon RDS

- Para usar AWS Backup para configurar backups contínuos para seu banco de dados do Amazon RDS, verifique se a permissão da API `rds:ModifyDBInstance` existe na função do IAM definida pela configuração do seu plano de backup. Para restaurar os backups contínuos do Amazon RDS, é necessário adicionar a permissão `rds:RestoreDBInstanceToPointInTime` ao perfil do IAM que você enviou para o trabalho de restauração. É possível usar o `AWS Backup default service role` para realizar backups e restaurações.
- Para descrever o intervalo de horários disponíveis para point-in-time recuperação, AWS Backup ligue`rds:DescribeDBInstanceAutomatedBackupsAPI`. No AWS Backup console, você deve ter a permissão da `rds:DescribeDBInstanceAutomatedBackups` API em sua política gerenciada AWS Identity and Access Management (IAM). É possível usar as políticas gerenciadas `AWSBackupFullAccess` ou `AWSBackupOperatorAccess`. Ambas as políticas têm todas as permissões necessárias. Para obter mais informações, consulte Políticas gerenciadas do .

Períodos de retenção: quando você altera seu período de retenção de PITR, AWS Backup liga `ModifyDBInstance` e aplica essa alteração imediatamente. Se você tiver outras atualizações de configuração pendentes na próxima janela de manutenção, a alteração do período de retenção da PITR também aplicará essas atualizações de configuração imediatamente. Para obter mais informações, consulte `ModifyDBInstance` na Referência de API do Amazon Relational Database Service.

Cópias dos backups contínuos do Amazon RDS:

- Os trabalhos incrementais de cópia de snapshot são processados mais rapidamente do que os trabalhos completos de cópia de snapshot. Manter uma cópia de snapshot anterior até que o novo trabalho de cópia seja concluído pode reduzir a duração do trabalho de cópia. Se você optar por copiar snapshots de instâncias de banco de dados do RDS, é importante observar que a exclusão das cópias anteriores primeiro fará com que cópias de snapshot completas (em vez de incrementais) sejam feitas. Para obter mais informações sobre como otimizar a cópia, consulte Cópia incremental de snapshot no Guia do usuário do Amazon RDS
- Criação de cópias de backups contínuos do Amazon RDS — Você não pode criar cópias de backups contínuos do Amazon RDS porque, para o AWS Backup Amazon RDS, não é possível copiar registros de transações. Em vez disso, AWS Backup cria um instantâneo e o copia com a frequência especificada no plano de backup.

Restaurações: você pode realizar uma point-in-time restauração usando um AWS Backup ou o Amazon RDS. Para obter instruções AWS Backup do console, consulte Restauração de um banco de dados do Amazon RDS. Para obter instruções do Amazon RDS, consulte Restaurar uma instância de banco de dados para horário especificado no Guia do usuário do Amazon RDS.

> **Tip**
>
> Uma instância de banco de dados com várias AZ (zona de disponibilidade) definida como não `Always On` deve ter uma retenção de backup definida como zero. Se ocorrerem erros, use o AWS CLI comando `disassociate-recovery-point` em vez de `delete-recovery-point`, em seguida, altere a configuração de retenção para 1 nas configurações do Amazon RDS.

Para obter informações gerais sobre como trabalhar com o Amazon RDS, consulte o Guia do usuário do Amazon RDS.

Aurora

Para habilitar o backup contínuo de seus recursos do Aurora, consulte as etapas na primeira seção desta página.

O procedimento para restaurar um cluster do Aurora para um ponto no tempo é uma variação das etapas para restaurar um snapshot de um cluster do Aurora.

Quando você realiza uma restauração pontual, o console exibe uma seção de tempo de restauração. Consulte Restaurar um backup contínuo mais abaixo nesta página em Trabalhar com backups contínuos.

SAP HANA em instâncias do Amazon EC2

Você pode fazer backups contínuos, que podem ser usados com point-in-time restauração (PITR) (observe que os backups sob demanda preservam os recursos no estado em que são usados; enquanto o PITR usa backups contínuos que registram as alterações durante um período de tempo).

Com backups contínuos, é possível restaurar seu banco de dados do SAP HANA em uma instância do EC2 retornando-o para um horário específico de sua escolha, com precisão de 1 segundo (retrocesso máximo de 35 dias). O backup contínuo funciona criando primeiramente um backup completo do seu recurso e, em seguida, fazendo backup constante dos logs de transações do

recurso. A restauração da PITR funciona acessando seu backup completo e reproduzindo o registro de transações até o momento em que você solicita AWS Backup a recuperação.

Você pode optar por backups contínuos ao criar um plano de backup AWS Backup usando o AWS Backup console ou a API.

Como habilitar os backups contínuos usando o console

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Planos de backup e, depois, escolha Criar plano.
3. Em Regras de backup, escolha Adicionar regra de backup.
4. Na seção Configuração da regra de backup, selecione Habilitar backups contínuos para recursos compatíveis.

Depois de desativar a PITR (point-in-timerestauração) para backups do banco de dados SAP HANA, os registros continuarão sendo enviados AWS Backup até que o ponto de recuperação expire (status igual a). `EXPIRED`) É possível mudar para um local alternativo de backup de logs no SAP HANA para interromper a transmissão de logs para o AWS Backup.

Um ponto de recuperação contínuo com um status de `STOPPED` indica que um ponto de recuperação contínuo foi interrompido; ou seja, os registros transmitidos do SAP HANA para AWS Backup aquele mostram que as alterações incrementais em um banco de dados têm uma lacuna. Os pontos de recuperação que ocorrerem dentro desse intervalo de tempo terão um status de `STOPPED`..

Para problemas que você possa encontrar durante os trabalhos restauração de backups contínuos (pontos de recuperação), consulte a seção de Solução de problemas de restauração do SAP HANA deste guia.

Encontrar um backup contínuo

Você pode usar o AWS Backup console para encontrar seu backup contínuo.

Para encontrar um backup contínuo usando o AWS Backup console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Cofres de backup e escolha o cofre de backup na lista.
3. Na seção Backups, na coluna Tipo de backup, classifique por pontos de recuperação Contínuos. Também é possível classificar pelo ID do ponto de recuperação para o prefixo Contínuo.

Restaurar um backup contínuo

Para restaurar um backup contínuo usando o AWS Backup console

- Durante o processo de restauração da PITR, o AWS Backup console exibe uma seção Tempo de restauração. Nesta seção, siga um destes procedimentos:
  - Escolha restaurar para o Último momento restaurável.
  - Escolha Especificar data e hora para inserir sua própria data e hora dentro do período de retenção.

Para restaurar um backup contínuo usando a AWS Backup API

1. Para o Amazon S3, consulte Usar a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do S3.
2. Para o Amazon RDS, consulte Usar a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do Amazon RDS.

Interromper ou excluir backups contínuos

Você pode interromper a criação de backups contínuos ou excluir backups específicos (point-in-time-recovery ou pontos PITR).

Se você quiser interromper os backups contínuos, exclua a regra de backup contínuo do plano de backup. Se você quiser interromper os backups contínuos de um ou mais recursos, mas não de todos os recursos, crie um plano de backup com a regra de backup contínuo para os recursos dos quais você ainda deseja fazer backup contínuo. Se, em vez disso, você excluir somente um ponto de recuperação de backup contínuo do seu cofre de backup, o plano de backup continuará executando a regra de backup contínuo, criando um ponto de recuperação.

No entanto, mesmo depois de excluir sua regra de backup contínuo, AWS Backup lembra o período de retenção da regra de backup agora excluída. Ele excluirá automaticamente o ponto de recuperação de backup contínuo do seu cofre de backup com base no período de retenção especificado.

Ao excluir pontos de recuperação do Amazon RDS, considere:

- Uma instância de banco de dados com várias AZ (zona de disponibilidade) definida como não `Always 0`n deve ter uma retenção de backup definida como zero. Se ocorrerem erros, use o

AWS CLI comando `disassociate-recovery-point` em vez de `edelete-recovery-point`, em seguida, altere a configuração de retenção para 1 nas configurações do Amazon RDS.

- Quando um ponto de point-in-time recuperação (um backup criado pelo backup contínuo) para o Amazon RDS é excluído, uma reinicialização do banco de dados é acionada e os registros binários são desativados. Para obter mais detalhes, consulte Período de retenção de backup no Guia do usuário do Amazon RDS.

Ao excluir pontos de recuperação do Aurora, considere:

Se isso for selecionado para um ponto de recuperação do Amazon Aurora, AWS Backup defina o período de retenção como 1 dia. Os backups do Aurora não podem ser completamente excluídos até que o cluster de origem também tenha sido excluído.

Cópia de backups contínuos

Se uma regra de backup contínuo também especificar uma cópia entre contas ou entre regiões, o AWS Backup tirará um snapshot do backup contínuo e copiará esse snapshot no cofre de destino. Para saber mais sobre como copiar seus pontos de recuperação entre contas e regiões, consulte Copiar um backup.

Os backups contínuos criam backups periódicos de acordo com a frequência definida na regra do plano de backup na conta e/ou região de destino.

AWS Backup não oferece suporte a cópias sob demanda de backups contínuos.

Alterar o período de retenção

Você pode usar AWS Backup para aumentar ou diminuir o período de retenção de sua regra de backup contínuo existente. O período mínimo de retenção é de 1 dia. O período máximo de retenção é de 35 dias.

Se você aumentar o período de retenção, o efeito será imediato. Se você diminuir o período de retenção, AWS Backup esperará até que passe tempo suficiente antes de aplicar a alteração para se proteger contra a perda de dados. Por exemplo, se você diminuir seu período de retenção de 35 dias para 20, AWS Backup continuará preservando 35 dias de backup contínuo até que tenham passado 15 dias. Esse design protege seus últimos 15 dias de backups no momento em que você fez a alteração.

Remover a única regra de backup contínuo de um plano de backup

Quando você cria um plano de backup com uma regra de backup contínuo e depois remove essa regra, AWS Backup lembra o período de retenção da sua regra agora excluída. Ele excluirá o backup contínuo do seu cofre de backup quando o período de retenção expirar.

Backups contínuos sobrepostos no mesmo recurso

Em geral, você deve proteger cada recurso com, no máximo, uma regra de backup contínuo. Isso ocorre porque backups contínuos adicionais são redundantes. No entanto, à medida que você expande sua propriedade de backup, é possível que vários planos, regras e cofres de backup se sobreponham em um único recurso. AWS Backup lida com essas sobreposições da seguinte maneira.

Se você incluir o mesmo recurso em mais de um plano de backup com uma regra de backup contínuo, só AWS Backup criará um backup contínuo para o primeiro plano de backup avaliado. Ele criará backups de snapshot para todos os outros planos de backup.

Se você incluir várias regras de backup contínuo em um único plano de backup:

- Se suas regras apontarem para o mesmo cofre de backup, criará AWS Backup apenas um backup contínuo para a regra com o período de retenção mais longo. Ele ignorará todas as outras regras.
- Se suas regras apontarem para cofres de backup diferentes, AWS Backup rejeita o plano como inválido.

Considerações sobre oint-in-time recuperação de P

Esteja ciente das seguintes considerações para point-in-time recuperação:

- Fallback automático para snapshots: se o AWS Backup não conseguir realizar um backup contínuo, ele tentará fazer um backup de snapshot.
- Não há suporte para backups contínuos sob demanda — AWS Backup não oferece suporte ao backup contínuo sob demanda porque o backup sob demanda registra um ponto no tempo, enquanto os registros de backup contínuo mudam com o passar do tempo.
- Não há compatibilidade com a transição para o armazenamento frio: os backups contínuos são incompatíveis com a transição para o armazenamento frio porque a transição para o armazenamento frio exige um período mínimo de transição de 90 dias, enquanto os backups contínuos têm um período máximo de retenção de 35 dias.

- Restauração de atividades recentes: a atividade do Amazon RDS permite restaurações até os últimos 5 minutos de atividade. O Amazon S3 permite restaurações até os últimos 15 minutos de atividade.

Backups do Amazon S3

AWS Backup suporta backup e restauração centralizados de aplicativos que armazenam dados somente no S3 ou junto com outros AWS serviços para banco de dados, armazenamento e computação. Muitos recursos estão disponíveis para backups do S3, incluindo o Backup Audit Manager.

Você pode usar uma única política de backup AWS Backup para automatizar centralmente a criação de backups dos dados do seu aplicativo. AWS Backup organiza automaticamente os backups em diferentes AWS serviços e aplicativos de terceiros em um local centralizado e criptografado (conhecido como cofre de backup) para que você possa gerenciar backups de todo o seu aplicativo por meio de uma experiência centralizada. Para o S3, você pode criar backups contínuos e restaurar os dados do aplicativo armazenados no S3 e restaurar os backups em um point-in-time único clique.

Com AWS Backup, você pode criar os seguintes tipos de backups de seus buckets do S3, incluindo dados de objetos, tags, listas de controle de acesso (ACLs) e metadados definidos pelo usuário:

- Os backups contínuos permitem que você restaure para a qualquer ponto no tempo dentro dos últimos 35 dias. Os backups contínuos para um bucket do S3 só devem ser configurados em um plano de backup.

  Consulte recuperação para um ponto no tempo para obter uma lista de serviços compatíveis e instruções sobre como usar o AWS Backup para fazer backups contínuos.
- Os backups periódicos usam snapshots de seus dados para permitir que você retenha dados pela duração especificada até 99 anos. É possível programar backups periódicos em frequências como uma hora, 12 horas, um dia, uma semana ou um mês. O AWS Backup fará backups periódicos durante a janela de backup que você definir no seu plano de backup.

  Consulte Criação de um plano de backup para entender como AWS Backup aplicar seu plano de backup aos seus recursos.

Cópias entre contas e regiões estão disponíveis para backups do S3, mas as cópias de backups contínuos não têm point-in-time recursos de restauração.

Os backups contínuos e periódicos dos buckets do S3 devem residir no mesmo cofre de backup.

Para os dois tipos de backup, o primeiro backup será completo, enquanto os backups subsequentes serão incrementais no nível do objeto.

> **Note**
>
> Você deve habilitar o versionamento do S3 em seu bucket do S3 para usar no Amazon AWS Backup S3. Mantivemos esse pré-requisito porque na AWS recomendamos o versionamento do S3 como uma melhor prática para a proteção de dados.
> Recomendamos que você defina um período de expiração do ciclo de vida para suas versões do S3. Não configurar um período de expiração do ciclo de vida pode aumentar seus custos do S3 porque AWS Backup faz backup e armazena todas as versões não expiradas dos seus dados do S3. Para saber mais sobre como configurar as políticas de ciclo de vida do S3, siga as instruções nesta página.

Comparar tipos de backup do S3

Sua estratégia de backup para recursos do S3 pode envolver apenas backups contínuos, backups periódicos (de snapshot) ou uma combinação de ambos. As informações abaixo podem ajudar você a escolher o que funciona melhor para sua organização:

Somente backups contínuos:

- Após a conclusão do primeiro backup completo dos dados existentes, as alterações nos dados do bucket do S3 serão rastreadas à medida que ocorrerem.
- As alterações monitoradas permitem que você use a PITR (point-in-time restauração) durante o período de retenção do backup contínuo. Para executar um trabalho de restauração, escolha o momento para o qual deseja fazer a restauração.
- O período de retenção de cada backup contínuo tem, no máximo, 35 dias.

Somente backups periódicos (de snapshot), programados ou sob demanda:

- AWS Backup verifica todo o bucket do S3, recupera a ACL e as tags de cada objeto e inicia uma solicitação Head para cada objeto que estava no snapshot anterior, mas não foi encontrado no snapshot que está sendo criado.
- O backup é point-in-time consistente.

- A data e a hora de backup registradas são a hora em que a travessia do bucket é AWS Backup concluída, não a hora em que uma tarefa de backup foi criada.
- O primeiro backup de um bucket é um backup completo. Cada backup subsequente é incremental, representando a alteração nos dados desde o último snapshot.
- O snapshot feito pelo backup periódico pode ter um período de retenção de até 99 anos.

Backups contínuos combinados com backups periódicos/de snapshot:

- Após o primeiro backup completo dos dados existentes (cada backup é completo), as alterações no bucket serão rastreadas à medida que ocorrerem.
- Você pode realizar uma point-in-time restauração a partir de um ponto de recuperação contínuo.
- Os instantâneos são point-in-time consistentes.
- Os snapshots são obtidos diretamente do ponto de recuperação contínua, eliminando a necessidade de verificar novamente um bucket para permitir processos mais rápidos.
- Os snapshots e os pontos de recuperação contínuos compartilham a linhagem de dados; o armazenamento de dados entre o snapshot e os pontos de recuperação contínuos não é duplicado.

Classes de armazenamento S3 compatíveis

AWS Backup permite que você faça backup dos dados do S3 armazenados nas seguintes classes de armazenamento do S3:

- S3 Standard
- S3 Standard - Acesso infrequente (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering (S3 INT)

Os backups de um objeto na classe de armazenamento S3 Intelligent-Tiering (INT) acessam esses objetos. Esse acesso aciona o S3 Intelligent-Tiering para mover automaticamente esses objetos para o Acesso Frequente.

Os backups que acessam os níveis de acesso infrequente, incluindo as classes S3 Standard - Acesso infrequente (IA) e S3 One Zone-IA, ficam sob a taxa de armazenamento do S3 do Acesso Frequente (aplica-se aos níveis Acesso Infrequente ou Acesso Instantâneo ao Arquivamento).

Com exceção do Glacier Instant Retrieval, as classes de armazenamento arquivado não são suportadas.

Para obter mais informações sobre preços de armazenamento para o Amazon S3, consulte Preços do Amazon S3.

Considerações AWS Backup para o Amazon S3

Os seguintes pontos devem ser considerados ao fazer backup de recursos do S3:

- Suporte focado em metadados de objetos: AWS Backup suporta os seguintes metadados: tags, listas de controle de acesso (ACLs), metadados definidos pelo usuário, data de criação original e ID da versão. Também é possível restaurar todos os dados e metadados que tiveram backup feito, exceto a data de criação original, o ID da versão, a classe de armazenamento e as tags eletrônicas.
- Um nome de chave de objeto do S3 pode ser composto pela maioria das strings codificáveis em UTF-8. Os seguintes caracteres Unicode são permitidos: `#x9` | `#xA` | `#xD` | `#x20 to #xD7FF` | `#xE000 to #xFFFD` | `#x10000 to #x10FFFF`.

  Nomes de chaves de objeto que incluam caracteres que não estejam nessa lista podem ser excluídos dos backups. Para obter mais informações, consulte a Especificação W3C para caracteres.
- Transição de armazenamento frio: a política de gerenciamento AWS Backup do ciclo de vida permite que você defina o cronograma para a expiração do backup, mas a transição de armazenamento frio dos backups do S3 não é suportada atualmente.
- Os backups de buckets do S3 com várias versões do mesmo objeto que foram criados no mesmo segundo não são compatíveis no momento.
- Para backups periódicos, AWS Backup faça o possível para rastrear todas as alterações nos metadados do objeto. No entanto, se você atualizar uma tag ou ACL várias vezes em 1 minuto, talvez o AWS Backup não capture todos os estados intermediários.
- AWS Backup atualmente não oferece suporte para backups de objetos criptografados com SSE-C. AWS Backup também não oferece suporte atualmente a backups de configurações de bucket, incluindo política, configurações, nome ou ponto de acesso do bucket.

- AWS Backup atualmente não oferece suporte a backups do S3 ativado. AWS Outposts

> **Important**
>
> Nas contas que registram eventos de leitura de dados, os buckets do S3 com CloudTrail registros ativados precisam que seus registros de acesso sejam salvos em um bucket de destino diferente; se CloudTrail os registros forem salvos no mesmo bucket que eles registram, um loop infinito se forma. Esse loop pode gerar cobranças inesperadas e indesejadas.
> Para obter mais informações, consulte Eventos de dados no Guia CloudTrail do usuário.

Janelas de conclusão de backup do S3

A tabela abaixo mostra exemplos de buckets de vários tamanhos para ajudar você a orientar as estimativas do tempo de conclusão do backup completo inicial de um bucket S3. Os tempos de backup variam de acordo com o tamanho, o conteúdo e as configurações de cada bucket.

Tamanho do bucket	Número de objetos	Tempo estimado para a conclusão do backup inicial
425 GB (gigabytes)	135 milhões	31 horas
800 TB (terabytes)	670 milhões	38 horas
6 PB (petabytes)	5 bilhões	100 horas
370 TB (terabytes)	7,5 bilhões	180 horas

Permissões e políticas para backup e restauração do Amazon S3

Para fazer backup, copiar e restaurar recursos do S3, é necessário ter as políticas corretas em seu perfil. Para adicionar essas políticas, acesse políticas gerenciadas da AWS. Adicione a AWSBackupServiceRolePolicyForS3Backupe AWSBackupServiceRolePolicyForS3Restoreàs funções que você pretende usar para fazer backup e restaurar buckets do S3.

Se você não tiver permissão suficiente, solicite ao gerente da conta administrativa (administrador) da sua organização que adicione as políticas aos perfis pretendidos.

Para obter mais informações, consulte Políticas gerenciadas e em linha no Guia do usuário do IAM.

AWS Backup para o S3 depende do recebimento de eventos do S3 pela Amazon. EventBridge Se essa configuração estiver desabilitada nas configurações de notificação do bucket do S3, os backups contínuos serão interrompidos para esses buckets com a configuração desabilitada. Para obter mais informações, consulte Usando EventBridge.

Práticas recomendadas e considerações de custo para backups do S3

Práticas recomendadas

Para buckets com mais de 300 milhões de objetos:

- Para buckets com mais de 300 milhões de objetos, a taxa de backup pode atingir até 17.000 objetos por segundo durante o backup inicial completo do bucket (os backups incrementais terão uma velocidade diferente). Os buckets contendo menos de 300 milhões de objetos fazem backup a uma taxa de cerca de 1.000 objetos por segundo.
- Os backups contínuos são recomendados.
- Se o ciclo de vida do backup for planejado para mais de 35 dias, também será possível habilitar os backups de snapshot para o bucket no mesmo cofre em que seus backups contínuos são armazenados.

Considerações de custo

- As políticas de ciclo de vida do S3 têm um recurso opcional chamado Excluir marcadores de exclusão de objetos expirados. Quando esse recurso está desativado, os marcadores de exclusão, às vezes na casa dos milhões, expiram sem um plano de limpeza. Quando o backup de buckets sem esse recurso é feito, dois problemas afetam o tempo e o custo:
  - Os marcadores de exclusão são copiados, assim como os objetos. O tempo de backup e o tempo de restauração podem ser afetados dependendo da proporção entre objetos e marcadores de exclusão.
  - Cada objeto e marcador que é copiado tem uma cobrança mínima. Cada marcador de exclusão é cobrado da mesma forma que um objeto de 128 KiB.
- Para contas que fazem backups pelo menos diariamente ou com mais frequência, é possível obter benefícios de custo com o uso de backups contínuos se os dados contidos nos backups tiverem alterações mínimas entre os backups.

- Os buckets maiores, que não mudam com frequência, podem se beneficiar de backups contínuos, pois isso pode resultar em custos mais baixos quando as digitalizações de todo o bucket, juntamente com várias solicitações por objeto, não precisam ser realizadas em objetos pré-existentes (objetos que não foram alterados em relação ao backup anterior).
- Os buckets que contêm mais de 100 milhões de objetos e que têm uma pequena taxa de exclusão em comparação com o tamanho geral do backup podem obter benefícios de custo com um plano de backup que contenha um backup contínuo com um período de retenção de 2 dias juntamente com de snapshots de uma retenção mais longa.
- O tempo de backup periódico (de snapshot) se alinha ao início do processo de backup quando não é necessária uma verificação do bucket. As verificações não são necessárias em um bucket que contém backups contínuos e de snapshots, pois nesses casos os snapshots são obtidos de um ponto de recuperação contínuo.
- Para cada objeto em um único S3-GIR (Amazon S3 Glacier Instant Retrieval), AWS Backup executa várias chamadas, o que resultará em cobranças de recuperação quando um backup for realizado.

  Custos de recuperação semelhantes se aplicam a buckets com objetos nas classes de armazenamento S3-IA e S3 One Zone-IA.
- AWS KMS, CloudTrail, e os CloudWatch recursos da Amazon que fazem parte de sua estratégia de backup podem resultar em custos adicionais além do armazenamento de dados do bucket S3. Veja a seguir para obter informações sobre como ajustar esse recursos:
  - Reduzir o custo do SSE-KMS com chaves de buckets do Amazon S3 no Guia do usuário do Amazon S3.
  - Você pode reduzir CloudTrail os custos excluindo AWS KMS eventos e desativando os eventos de dados do S3:
    - Excluir AWS KMS eventos: no Guia do CloudTrail usuário, a criação de uma trilha no console (seletores de eventos básicos) permite a opção de excluir AWS KMS eventos para filtrar esses eventos da sua trilha (a configuração padrão inclui todos os eventos do KMS):
    - A opção para registrar em log ou excluir eventos do KMS só estará disponível se você registrar em log eventos de gerenciamento em sua trilha. Se optar por não registrar em log eventos de gerenciamento, os eventos do KMS não serão registrados em log e não será possível alterar as configurações de log de eventos do KMS.
    - AWS KMS ações como`Encrypt`,`Decrypt`, e `GenerateDataKey` normalmente geram um grande volume (mais de 99%) de eventos. Agora essas ações são registradas em log como eventos de Leitura. As ações relevantes e de baixo volume do KMS, como `Disable`, `Delete`

e `ScheduleKey` (que normalmente representam menos de 0,5% do volume de eventos do KMS) são registradas em log como eventos de Gravação.

- Para excluir eventos de alto volume, como `Encrypt`, `Decrypt` e`GenerateDataKey`, mas ainda registrar em log eventos relevantes como `Disable`, `Delete` e `ScheduleKey`, opte por registrar eventos gerenciados de Gravação e desmarque a caixa de seleção para Excluir eventos do AWS KMS .
- Desabilitar eventos de dados do S3: por padrão, trilhas e armazenamentos de dados de eventos não registram em log eventos de dados. Desabilite os eventos de dados do S3 antes do backup inicial para reduzir custos.

- Para reduzir CloudWatch custos, você pode parar de enviar CloudTrail eventos para o CloudWatch Logs ao atualizar uma trilha para desativar as configurações do CloudWatch Logs.

Restaurar backups do S3

Você pode restaurar os dados do S3 que você fez backup usando AWS Backup para a classe S3 Standard Storage. É possível restaurar os dados do S3 em um bucket existente, incluindo o bucket original. Durante a restauração, também é possível criar um bucket do S3 como o destino da restauração. Você pode restaurar os backups do S3 somente no mesmo Região da AWS local em que seu backup está localizado.

É possível restaurar todo o bucket do S3 ou pastas ou objetos dentro do bucket. O AWS Backup restaura a versão atual desse objeto.

Para restaurar seus dados do S3 usando AWS Backup, consulteRestaurar dados do S3.

Backups de máquinas virtuais

AWS Backup oferece suporte à proteção de dados centralizada e automatizada para máquinas virtuais (VMs) VMware locais, juntamente com VMs no VMware Cloud™ (VMC) on e no VMware Cloud™ (VMC) on AWS . AWS Outposts Você pode fazer backup de suas máquinas virtuais locais e VMC para o. AWS Backup Em seguida, é possível restaurar do AWS Backup para VMs on-premises, VMs no VMC ou no VMC no AWS Outposts.

AWS Backup também fornece recursos de gerenciamento de backup de VM AWS nativos e totalmente gerenciados, como descoberta de VMs, agendamento de backup, gerenciamento de retenção, um nível de armazenamento de baixo custo, cópia entre regiões e entre contas, suporte para Vault Lock e AWS Backup Audit Manager, criptografia independente dos dados de origem AWS

Backup e políticas de acesso ao backup. Para obter uma lista completa dos recursos e dos detalhes, consulte a tabela Disponibilidade de recursos por recurso.

Você pode usar AWS Backup para proteger suas máquinas virtuais no VMware Cloud™ on. AWS Outposts AWS Backup armazena seus backups de VM no local Região da AWS ao qual seu VMware Cloud™ on está AWS Outposts conectado. Você pode usar AWS Backup para proteger seu VMware Cloud™ on AWS Backup VMs quando estiver usando o VMware Cloud™ on AWS Outposts para atender às suas necessidades locais de processamento de dados e de baixa latência para seus dados de aplicativos. Com base em seus requisitos de residência de dados, você pode AWS Backup optar por armazenar backups dos dados do seu aplicativo no pai Região da AWS ao qual o seu AWS Outposts está conectado.

VMs compatíveis

AWS Backup pode fazer backup e restaurar máquinas virtuais gerenciadas por um VMware vCenter.

Atualmente suportado:

- vSphere 8, 7.0 e 6.7
- Tamanhos de disco virtual que são múltiplos de 1 KiB
- Armazenamentos de dados NFS, VMFS e VSAN no local e no VMC em AWS
- Modos de transporte SCSI Hot-Add e Network Block Device Secure Sockets Layer (NBDSSL) para copiar dados das VMs de origem para o VMware local AWS
- Modo Hot-Add para proteger VMs no VMware Cloud on AWS

Atualmente não suportado:

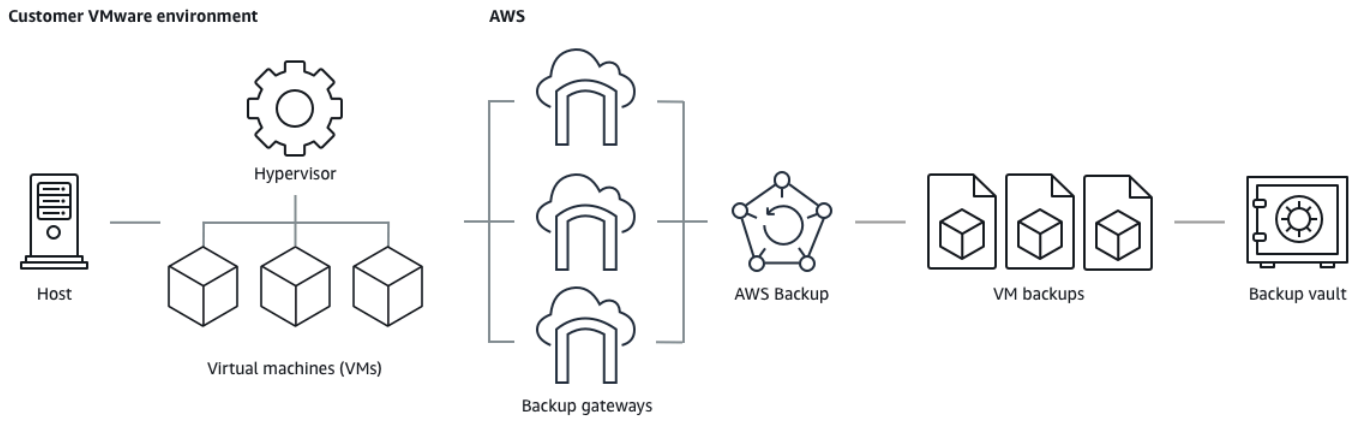
- Discos RDM (mapeamento de disco bruto) ou controladores NVMe e seus discos
- Modos de disco independente, persistente e independente, não persistente

Consistência de backup

O AWS Backup, por padrão, captura backups de VMs consistentes com aplicações usando a configuração de quietude do VMware Tools na VM. Seus backups serão consistentes com as aplicações se forem compatíveis com o VMware Tools. Se o recurso de quiescência não estiver disponível, AWS Backup captura backups consistentes com falhas. Valide que seus backups atendem às necessidades da sua organização testando suas restaurações.

Gateway de backup

O gateway de backup é um AWS Backup software disponível para download que você implanta em sua infraestrutura VMware para conectar suas VMs VMware. AWS Backup O Backup Gateway se conecta ao seu servidor de gerenciamento de VM para descobrir VMs, descobrir suas VMs, criptografar dados e transferir dados de forma eficiente para o AWS Backup. O diagrama a seguir mostra como o Backup Gateway se conecta às suas VMs:



Para baixar o software do gateway de backup, siga o procedimento para Trabalhar com gateways.

Para obter informações sobre endpoints VPC (Virtual Private Cloud), consulte AWS Backup e conectividade. AWS PrivateLink

O gateway de backup vem com sua própria API, que é mantida separadamente da API do AWS Backup . Para ver uma lista das ações da API do Backup Gateway, consulte Ações do Backup Gateway. Para ver uma lista dos tipos de dados da API do Backup Gateway, consulte Tipos de dados do Backup Gateway.

Endpoints

Os usuários existentes que atualmente usam um endpoint público e desejam mudar para um endpoint da VPC (Nuvem privada virtual) podem criar um gateway com um endpoint da VPC usando o AWS PrivateLink, associar o hipervisor existente ao gateway e, depois, excluir o gateway que contém o endpoint público.

Configurar sua infraestrutura para usar o gateway de backup

O gateway de backup requer as configurações de rede, firewall e hardware a seguir para fazer backup e restaurar suas máquinas virtuais.

Configuração de rede

O gateway de backup exige que determinadas portas tenham permissão para sua operação. Permita as seguintes portas:

1. Saída TCP 443
   - Origem: gateway de backup
   - Destino: AWS
   - Uso: permite que o gateway de Backup se comunique com AWS.
2. Entrada TCP 80
   - Fonte: O host que você usa para se conectar ao AWS Management Console
   - Destino: gateway de backup
   - Uso: por sistemas locais para obter a chave de ativação do gateway de backup. A porta 80 é usada somente durante a ativação do gateway de Backup. AWS Backup não exige que a porta 80 seja acessível ao público. O nível necessário de acesso à porta 80 depende da configuração da rede. Se você ativar seu gateway a partir do AWS Management Console, o host a partir do qual você se conecta ao console deve ter acesso à porta 80 do gateway.
3. Saída UDP 53
   - Origem: gateway de backup
   - Destino: Servidor Domain Name Service (DNS – Serviço do nome de domínio)
   - Uso: permite que o gateway de backup se comunique com o DNS.
4. Saída TCP 22
   - Origem: gateway de backup
   - Destino: AWS Support
   - Uso: Permite AWS Support acessar seu gateway para ajudá-lo com problemas. Não é necessário ter essa porta aberta para a operação normal do gateway, mas é necessária estar aberta para a solução de problemas.
5. Saída UDP 123
   - Origem: cliente NTP
   - Destino: servidor NTP
   - Uso: usada por sistemas locais para sincronizar a hora da máquina virtual com a hora do host.
6. Saída TCP 443
   - Origem: gateway de backup

- Destino: VMware vCenter
- Uso: permite que o gateway de backup se comunique com o VMware vCenter.

7. Saída TCP 443
   - Origem: gateway de backup
   - Destino: hosts do ESXi
   - Uso: permite que o gateway de backup se comunique com os hosts do ESXi.
8. Saída TCP 902
   - Origem: gateway de backup
   - Destino: hosts do VMware ESXi
   - Uso: usado para transferência de dados via gateway de backup.

As portas acima são necessárias para o gateway de Backup. Consulte Criação de um AWS Backup VPC endpoint para obter mais informações sobre como configurar endpoints da Amazon VPC para. AWS Backup

Configuração do firewall

O gateway de backup requer acesso aos seguintes endpoints de serviço para se comunicar Amazon Web Services. Se usar um firewall ou roteador para filtrar ou limitar o tráfego de rede, você deverá configurar o firewall e o roteador para permitir a comunicação externa com a AWS nesses endpoints de serviço. O uso de um proxy HTTP entre o gateway de backup e os pontos de serviço não é compatível.

```
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
```

Configure seu gateway para várias NICs na VMware

Você pode manter redes separadas para seu tráfego interno e externo conectando várias conexões de interface de rede virtual (NICs) ao seu gateway e, em seguida, direcionando o tráfego interno (gateway para hipervisor) e externo (gateway para) separadamente. AWS

Por padrão, as máquinas virtuais conectadas ao AWS Backup gateway têm um adaptador de rede (`eth0`). Essa rede inclui o hipervisor, as máquinas virtuais e o gateway de rede (gateway de Backup) que se comunica com a Internet mais ampla.

Veja um exemplo de configuração com várias interfaces de rede virtual:

```
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
```

- Neste exemplo, a conexão é com um hipervisor com IP `10.0.3.123`, o gateway usará `eth0` como o IP do hipervisor que faz parte do bloco `10.0.3.0/24`
- Para se conectar a um hipervisor com IP `10.0.0.234`, o gateway usará `eth1`
- Para se conectar a um IP fora das redes locais (por exemplo, `34.193.121.211`), o gateway retornará ao gateway padrão, `10.0.0.1`, que está no bloco `10.0.0.0/24` e, portanto, passará `eth1`

A primeira sequência para adicionar outro adaptador de rede ocorre no cliente vSphere:

1. No cliente VMware vSphere, abra o menu de contexto (clique com o botão direito) da máquina virtual do gateway e escolha Editar configurações.
2. Na guia Hardware virtual da caixa de diálogo Propriedades da máquina virtual, abra o menu Adicionar novo dispositivo e selecione Adaptador de rede para adicionar um novo adaptador de rede.
3.
   a. Expanda os detalhes da Nova rede para configurar o novo adaptador.
   b. Verifique se a opção Conectar ao ativar está selecionada.
   c. Em Tipo de adaptador, consulte Tipos de adaptador de rede na Documentação do ESXi e do vCenter Server.
4. Clique em OK para salvar as novas configurações do adaptador de rede.

A próxima sequência de etapas para configurar um adaptador adicional ocorre no console do AWS Backup gateway (observe que essa não é a mesma interface do console de AWS gerenciamento em que os backups e outros serviços são gerenciados).

Depois que a nova NIC for adicionada à VM do gateway, você precisará:

- Acessar `Command Prompt` e ligue os novos adaptadores
- Configurar IPs estáticos para cada nova NIC
- Definir a NIC preferencial como padrão

Para fazer isso:

1. No cliente VMware vSphere, selecione sua máquina virtual de gateway e inicie o Web Console para acessar o console local do gateway de Backup.
    - Para obter mais informações sobre como acessar um console local, consulte Acessar o console local do gateway com o VMware ESXi
2. Saia do prompt de comando e acesse Configuração de rede > Configurar IP estático e siga as instruções de configuração para atualizar a tabela de roteamento.
    a. Atribua um IP estático na sub-rede do adaptador de rede.
    b. Configure uma máscara de rede.
    c. Insira o endereço IP do gateway padrão. Esse é o gateway de rede que se conecta a todo o tráfego fora da rede local.
3. Selecione Definir adaptador padrão para designar o adaptador que será conectado à nuvem como o dispositivo padrão.
4. Todos os endereços IP do gateway podem ser exibidos no console local e na página de resumo da VM no VMware vSphere.

Requisitos de hardware

Você deve poder dedicar os seguintes recursos mínimos em um host de máquina virtual para o gateway de backup:

- Quatro processadores virtuais
- 8 GiB de memória RAM reservada

Permissões da VMware

Esta seção lista as permissões mínimas do VMware necessárias para uso. AWS Backup gateway Essas permissões são necessárias para que o gateway de Backup descubra, faça backup e restaure máquinas virtuais.

Para usar o gateway de backup com o VMware Cloud™ ativado AWS ou o VMware Cloud™ ativado AWS Outposts, você deve usar o usuário administrador padrão `cloudadmin@vmc.local` ou atribuir a CloudAdmin função ao seu usuário dedicado.

Para usar o Backup Gateway com máquinas virtuais locais da VMware, crie um usuário dedicado com as permissões listadas abaixo.

Global

- Desabilitar métodos
- Habilitar métodos
- Licenças
- Evento de log
- Gerenciar atributos personalizados
- Definir atributos personalizados

Marcação do vSphere

- Atribuir ou cancelar a atribuição da tag do vSphere

DataStore

- Alocar espaço
- Navegar pelo datastore
- Configurar datastore (para o datastore vSAN)
- Operações de arquivo de baixo nível
- Atualizar arquivos da máquina virtual

Host

- Configuração

- Configurações avançadas
- Configuração de partição de armazenamento

Pasta

- Criar pasta

Rede

- Atribuir rede

Grupo dvPort

- Criar
- Delete

Recurso

- Atribuir máquina virtual ao grupo de recursos

Máquina virtual

- Alterar a configuração
  - Adquirir concessão de disco
  - Adicionar disco existente
  - Adicionar novo disco
  - Configuração avançada
  - Alterar configurações do
  - Configurar dispositivo bruto
  - Modificar configurações do dispositivo
  - Remover disco
  - Definir anotação
  - Alternar monitoramento de alterações de disco
- Editar inventário

  - Criar a partir de um existente
  - Criar
  - Inscreva-se
  - Remover
  - Cancelar o registro
- Interação
  - Desligar
  - Ligar
- Provisionamento
  - Permitir acesso ao disco
  - Permitir acesso somente leitura ao disco
  - Permitir download da máquina virtual
- Gerenciamento do snapshot
  - Criar snapshot
  - Remover Snapshot
  - Reverter para snapshot

Trabalhar com gateways

Para fazer backup e restaurar suas máquinas virtuais (VMs) usando AWS Backup, você deve primeiro instalar um gateway de backup. Um gateway é um software na forma de um modelo OVF (Open Virtualization Format) que conecta o Amazon Web Services Backup ao seu hipervisor, permitindo que ele detecte automaticamente suas máquinas virtuais e permite que você faça backup e restaure elas.

Um único gateway pode executar até quatro trabalhos de backup ou de restauração ao mesmo tempo. Para executar mais de quatro trabalhos ao mesmo tempo, crie mais gateways e associe-os ao seu hipervisor.

Criar um gateway

Como criar um gateway:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, na seção Recursos externos, escolha Gateways.

3. Escolha Criar gateway.
4. Na seção Configurar gateway, siga estas instruções para baixar e implantar o modelo OVF.

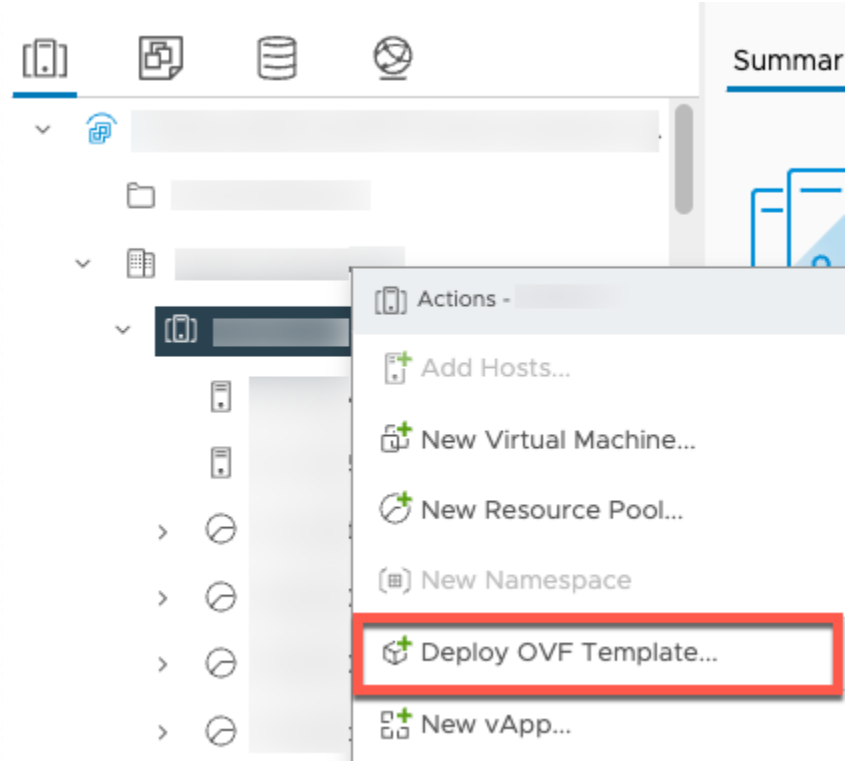
Baixar o software da VMware

Conectar o hipervisor

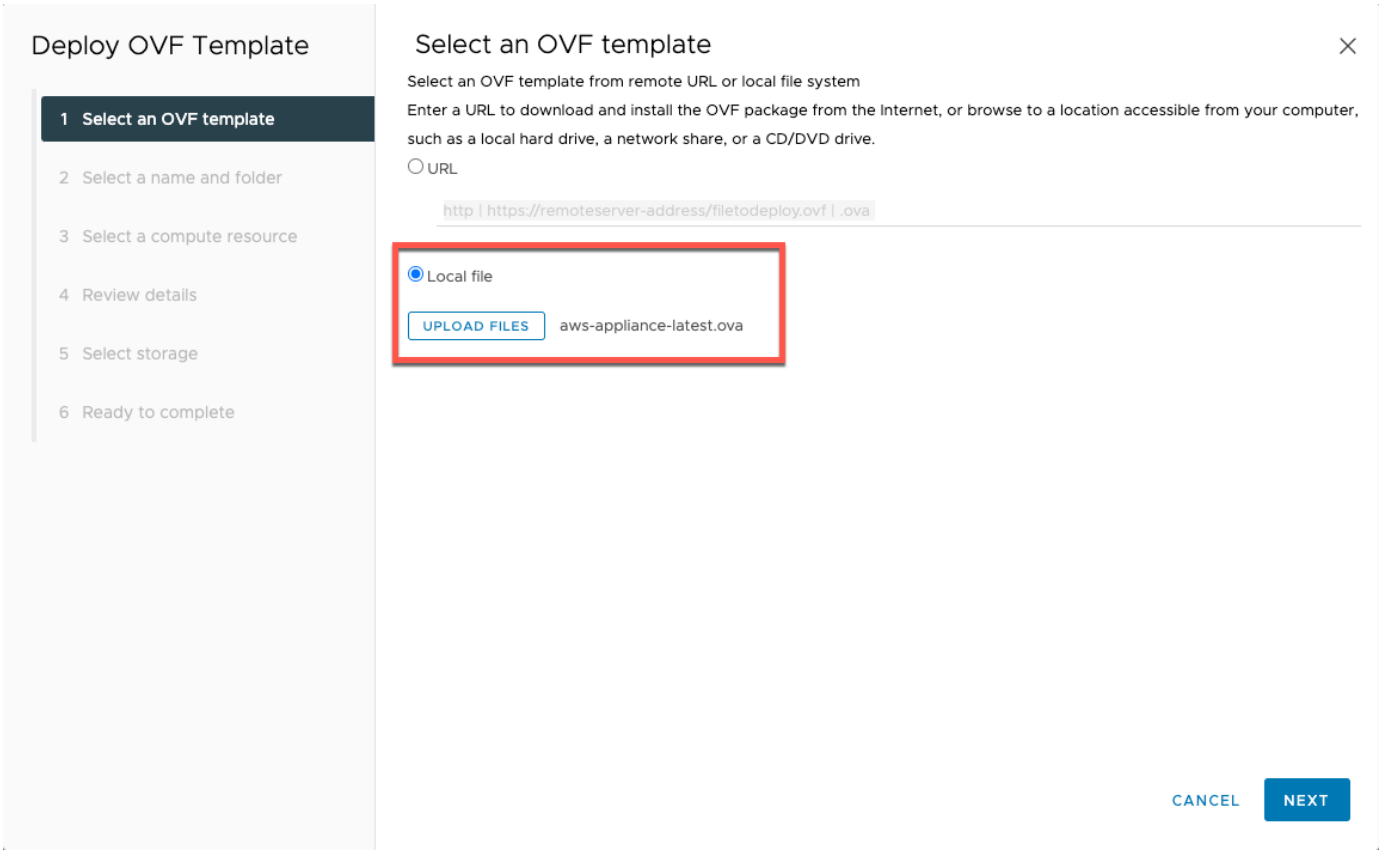
Os gateways se conectam AWS Backup ao seu hipervisor para que você possa criar e armazenar backups de suas máquinas virtuais. Para configurar seu gateway no VMware ESXi, baixe o modelo OVF. O download pode levar cerca de 10 minutos.

Depois de concluído, execute as seguintes etapas:

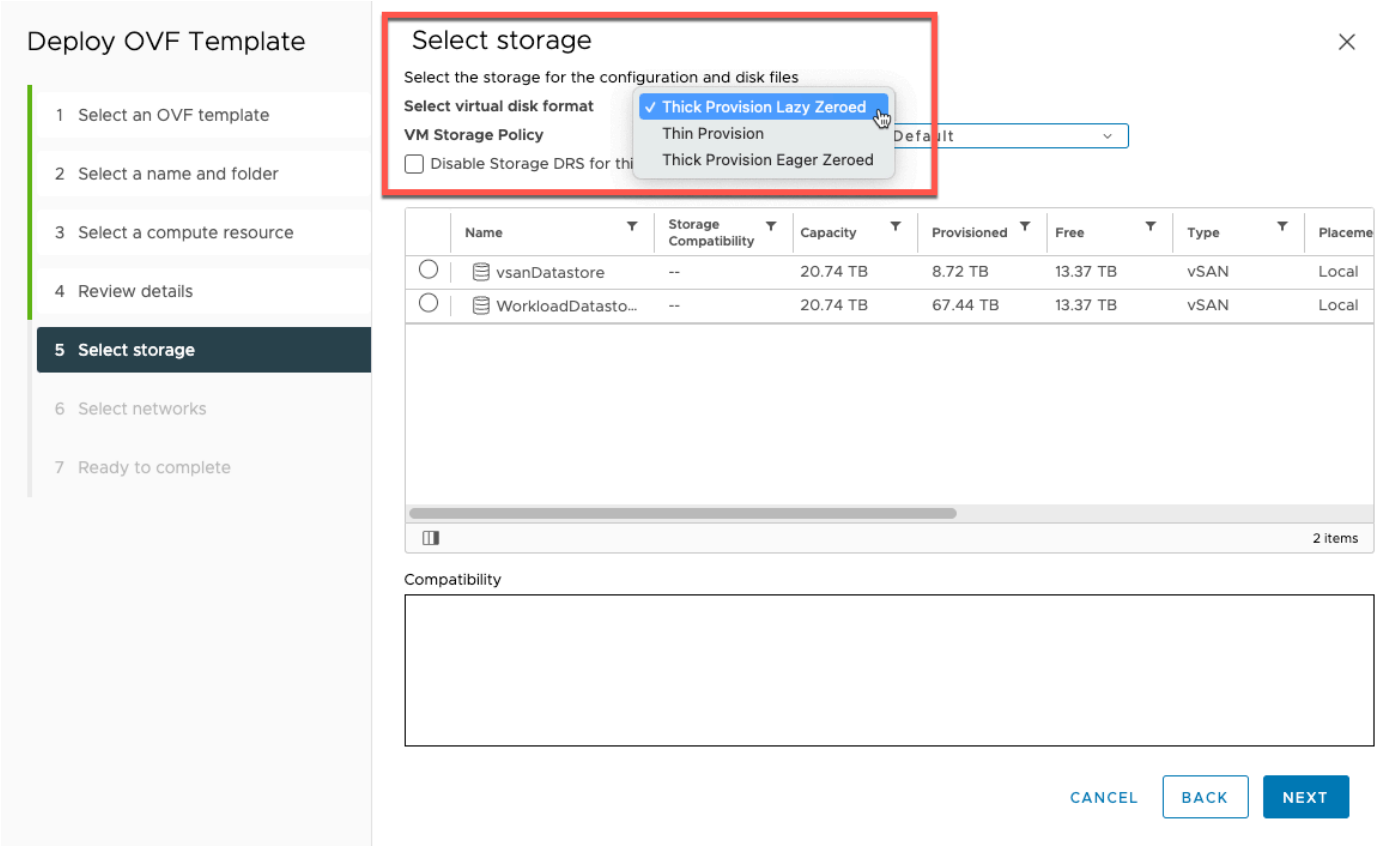
1. Conecte-se ao hipervisor da sua máquina virtual usando o VMware vSphere.
2. Clique com o botão direito do mouse em um objeto pai de uma máquina virtual e selecione Implantar modelo OVF.



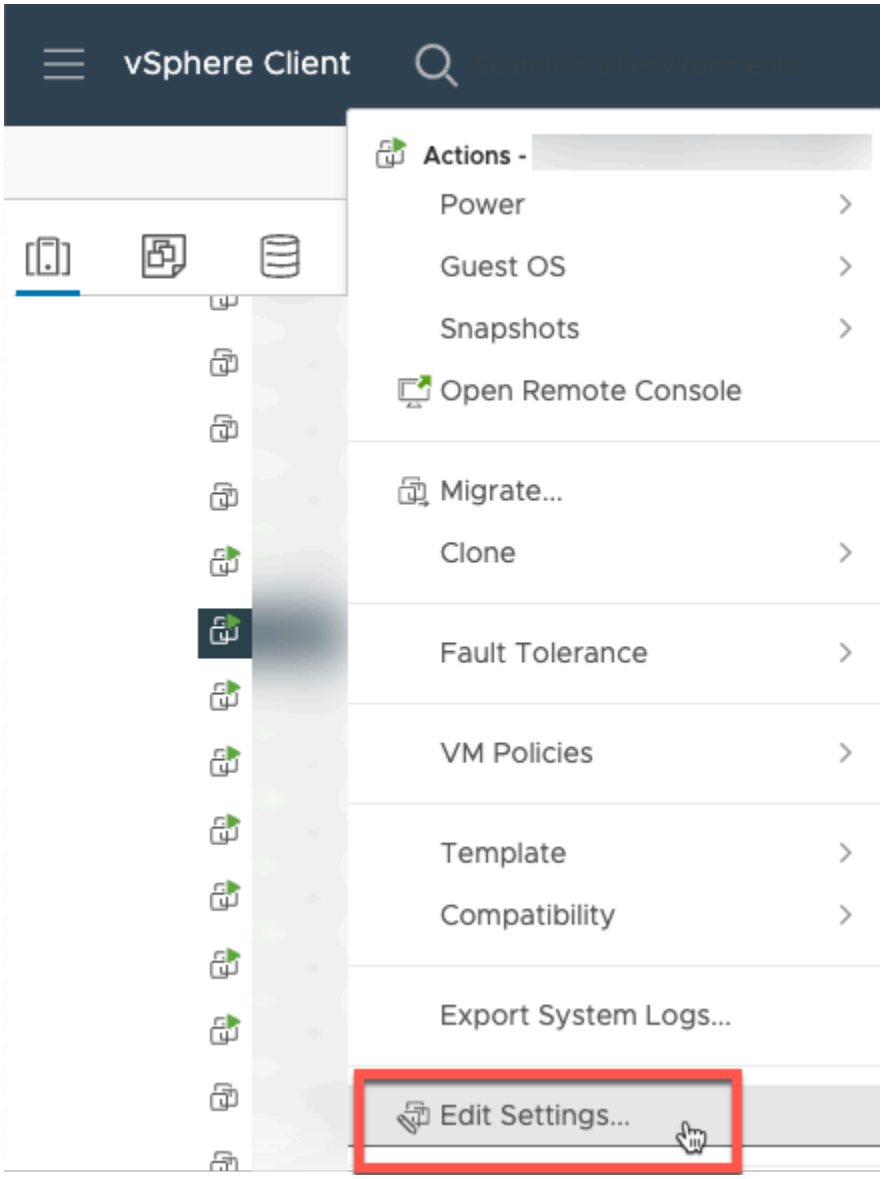
3. Escolha Arquivo local e faça o upload do aws-appliance-latestarquivo.ova que você baixou.



4. Siga as etapas do assistente de implantação para implantá-lo. Na página Selecionar armazenamento, selecione o formato de disco virtual Thick Provision Lazy Zeroed.

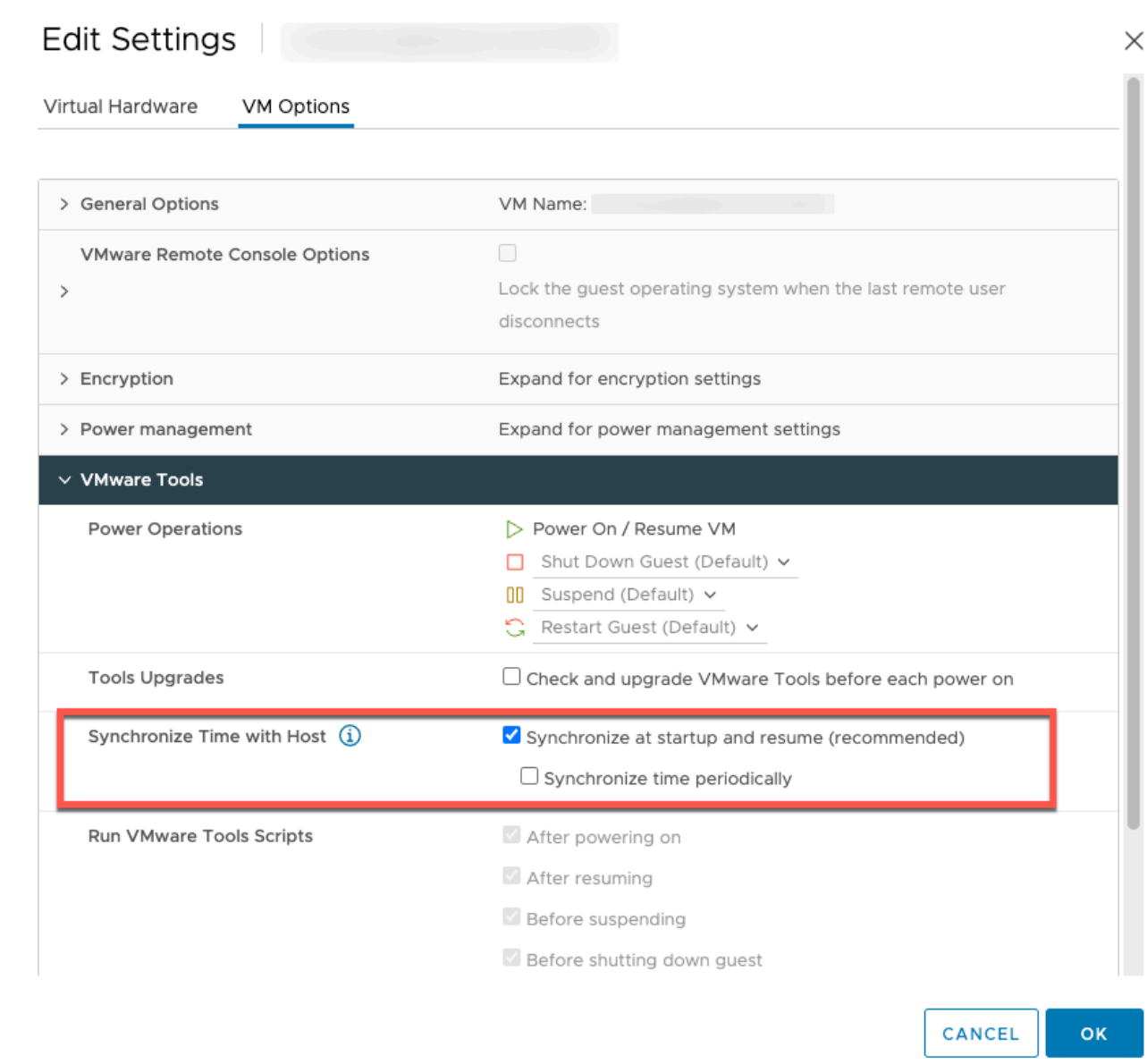


5. Depois de implantar o OVF, clique com o botão direito do mouse no gateway e escolha Editar configurações.

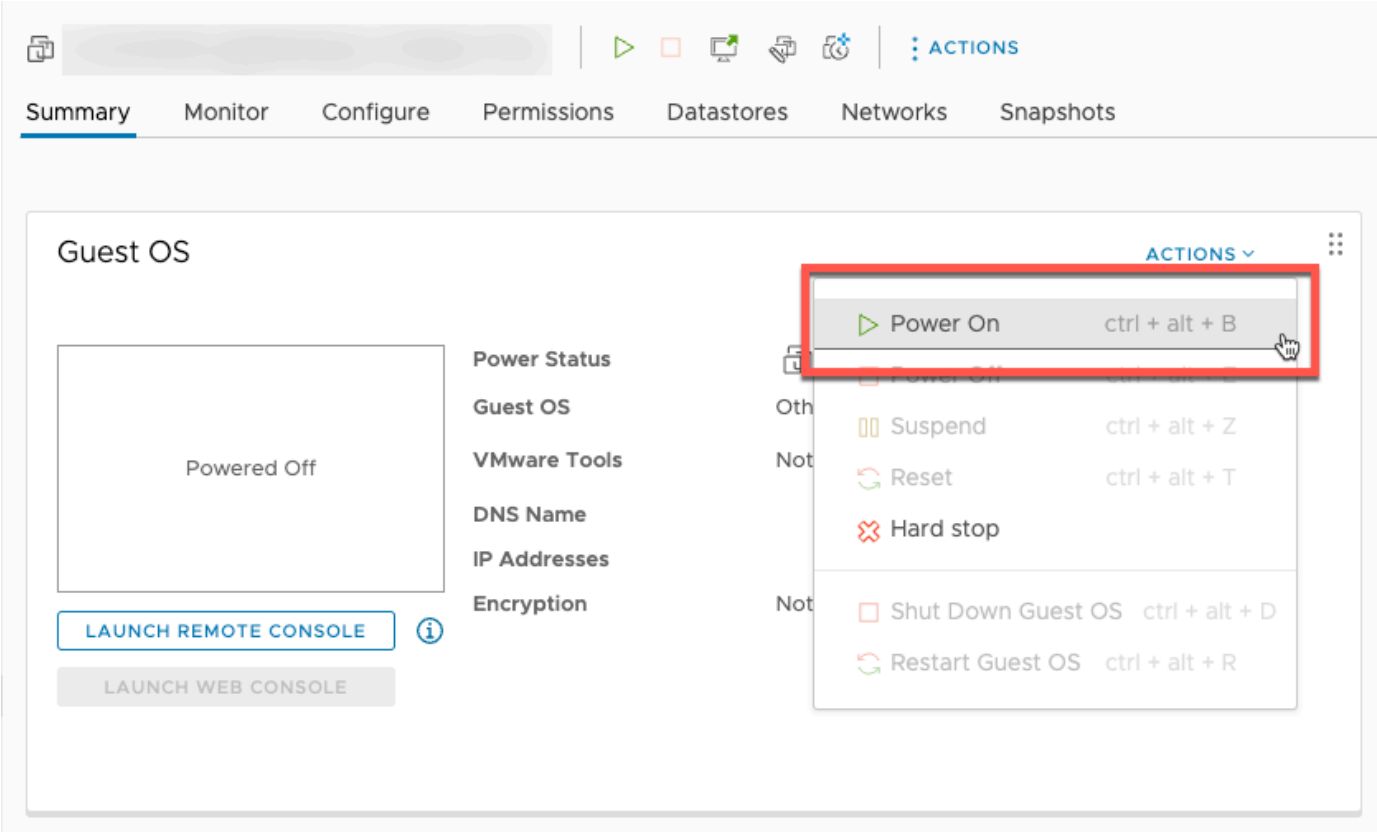


a. Em Opções da VM, acesse Ferramentas da VM.

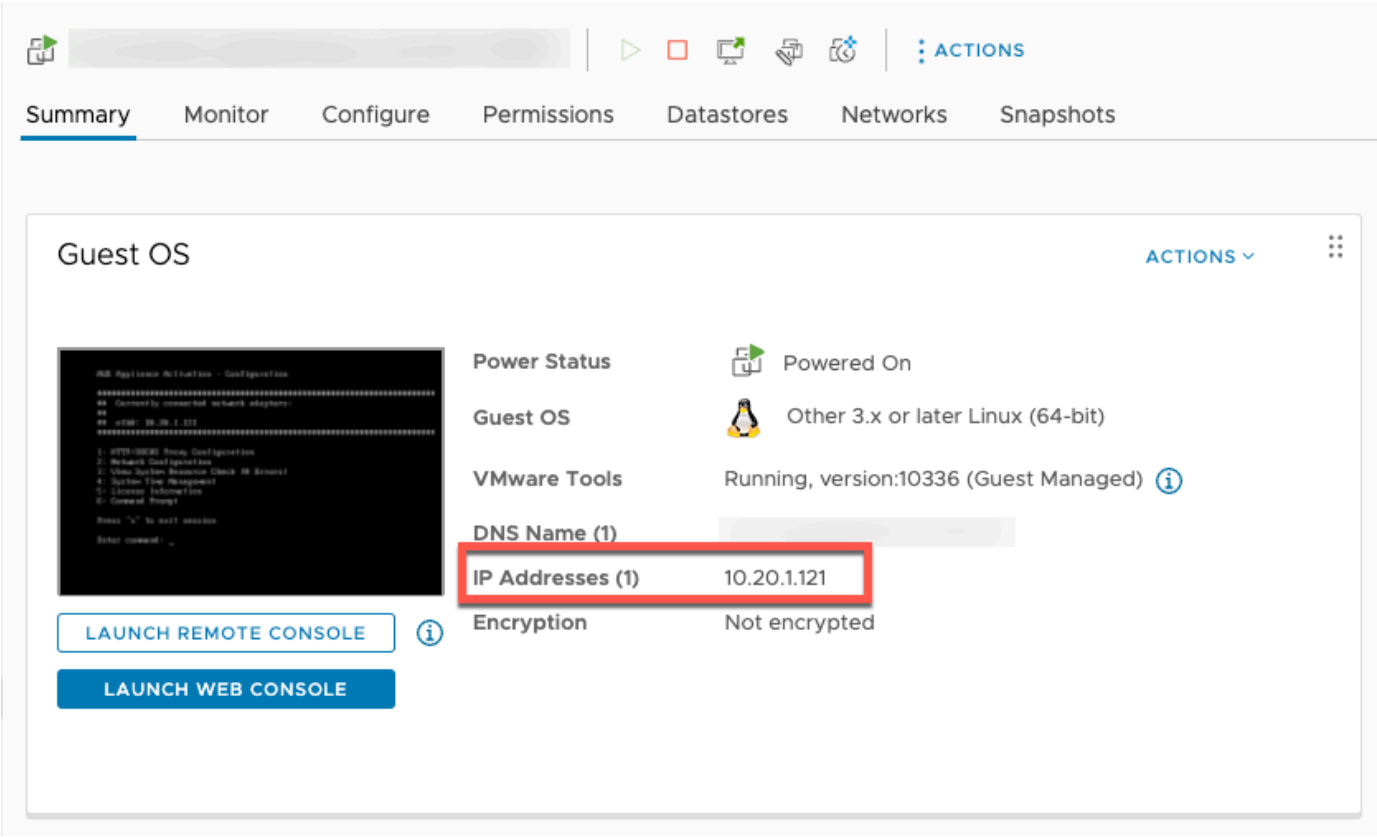
b. Verifique se em Sincronizar hora com o host, a opção Sincronizar na inicialização e na retomada está selecionada.



6. Ative a máquina virtual selecionando “Ativar” no menu Ações.



7. Copie o endereço IP do resumo da VM e insira-o abaixo.



Depois de fazer o download do software da VMWare, conclua as etapas a seguir:

1. Na seção Conexão do gateway, digite o endereço IP do gateway.
   a. Para encontrar esse endereço IP, acesse o vSphere Client.
   b. Selecione seu gateway na guia Resumo.
   c. Copie o endereço IP e cole-o na barra de texto do AWS Backup console.
2. Na seção Configurações do gateway,
   a. digite o nome do Gateway.
   b. Verifique a AWS região.
   c. Escolha se o endpoint será acessível publicamente ou hospedado com sua nuvem privada virtual (VPC).
   d. Dependendo do endpoint escolhido, insira o nome DNS do endpoint da VPC.

      Para obter mais informações, consulte Criar um endpoint da VPC.
3. [Opcional] Na seção Tags do Gateway, você pode atribuir tags inserindo a chave e o valor opcional. Para adicionar mais de uma tag, clique em Adicionar outra tag.
4. Para concluir o processo, clique em Criar gateway, que levará você à página de detalhes do gateway.

Editar ou excluir um gateway

Como editar ou excluir um gateway:

1. No painel de navegação esquerdo, na seção Recursos externos, escolha Gateways.
2. Na seção Gateways, escolha um gateway pelo nome do gateway.
3. Para editar o nome do gateway, escolha Editar.
4. Para excluir o gateway, escolha Excluir e, depois, escolha Excluir gateway.

   Não é possível reativar um gateway excluído. Caso queira se conectar ao hipervisor novamente, siga o procedimento em Criar um gateway.
5. Para se conectar a um hipervisor, na seção Hipervisor conectado, escolha Conectar.

Cada gateway se conecta a um único hipervisor. No entanto, é possível conectar vários gateways ao mesmo hipervisor para aumentar a largura de banda entre eles além da do primeiro gateway.

6. Para atribuir, editar ou gerenciar tags, na seção Tags, escolha Gerenciar tags.

Limitação da largura de banda do gateway de backup

> **Note**
>
> Esse recurso foi disponibilizado em novos gateways implantados após 15 de dezembro de 2022. Para os gateways existentes, esse novo recurso foi disponibilizado por meio de uma atualização automática de software em 30 de janeiro de 2023 ou antes dessa data. Para atualizar o gateway para a versão mais recente manualmente, use o AWS CLI comando `UpdateGatewaySoftwareNow`.

Você pode limitar a taxa de transferência de upload do seu gateway para controlar AWS Backup a quantidade de largura de banda de rede que o gateway usa. Por padrão, um gateway ativado não tem limites para taxas.

Você pode configurar um cronograma de limite de taxa de largura de banda usando o AWS Backup console ou usando a API por meio do AWS CLI (). `PutBandwidthRateLimitSchedule` Ao usar uma programação de limite de taxa de largura de banda, é possível configurar limites para serem alterados automaticamente ao longo do dia ou da semana.

A limitação da taxa de largura de banda funciona equilibrando o throughput de todos os dados que estão tendo upload feito, calculada em média a cada segundo. Embora seja possível que os uploads ultrapassem brevemente o limite da taxa de largura de banda por um determinado micro ou milissegundo, isso normalmente não resulta em grandes picos por longos períodos.

É possível adicionar um máximo de 20 intervalos. O valor máximo da taxa de upload é de 8 milhões de megabytes por segundo (Mbps).

Visualize e edite o cronograma de limite de taxa de largura de banda para seu gateway usando o console. AWS Backup

Esta seção descreve como visualizar e editar a programação de limite de taxa de largura de banda para o gateway.

Como visualizar e editar a programação do limite da taxa de largura de banda

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação à esquerda, escolha Gateways. No painel Gateways, os gateways são exibidos por nome. Clique no botão de opção ao lado do nome do gateway que você deseja gerenciar.
3. Depois de selecionar um botão de opção, o menu suspenso Ação ficará disponível para clicar. Clique em Ações e, depois, clique em Editar programação do limite da taxa de largura de banda. A programação atual será exibida. Por padrão, um gateway novo ou não editado não tem limites de taxa de largura de banda definidos.

   > **Note**
   >
   > Também é possível clicar em Gerenciar programação na página de detalhes do gateway para navegar até a página Editar largura de banda.

4. (Opcional) Escolha Adicionar intervalo para adicionar um novo intervalo configurável à programação. Para cada intervalo, insira as seguintes informações:

   a. Dias da semana: selecione o dia ou os dias recorrentes nos quais você deseja aplicar o intervalo. Depois de escolhidos, os dias serão exibidos abaixo do menu suspenso. É possível removê-los clicando no X ao lado do dia.

   b. Hora de início: insira a hora de início do intervalo de largura de banda, usando o formato HH:MM de 24 horas. A hora é renderizada em Tempo Universal Coordenado (UTC).

      Nota: Seu bandwidth-rate-limit intervalo começa no início do minuto especificado.

   c. Hora de término: insira a hora de término do intervalo de largura de banda, usando o formato HH:MM de 24 horas. A hora é renderizada em Tempo Universal Coordenado (UTC).

      > **Important**
      >
      > O bandwidth-rate-limit intervalo termina no final do minuto especificado. Para agendar um intervalo que termine no final de uma hora, insira 59. Para programar intervalos contínuos consecutivos, fazendo a transição no início da hora, sem interrupção entre os intervalos, insira 59 para o minuto final do primeiro intervalo. Insira `00` para o minuto inicial do intervalo seguinte.

d. Taxa de upload: insira o limite da taxa de upload, em megabits por segundo (Mbps). O valor mínimo é de 102 megabytes por segundo (Mbps).

5. (Opcional) Repita a etapa anterior conforme desejado até que sua programação de limite de taxa de largura de banda seja concluída. Se precisar excluir um intervalo da sua agenda, escolha Remover.

> **Important**
>
> Os intervalos de limite de taxa de largura de banda não podem se sobrepor. A hora de início de um intervalo deve ocorrer após a hora de término de um intervalo anterior e antes da hora de início de um intervalo seguinte. A hora de término deve ocorrer antes da hora de início do intervalo seguinte.

6. Quando terminar, clique no botão Salvar alterações.

Visualize e edite a programação de limite de taxa de largura de banda para seu gateway usando a AWS CLI.

A ação `GetBandwidthRateLimitSchedule` pode ser usada para visualizar a programação do controle de utilização de largura de banda para um gateway especificado. Se não houver uma programação definida, ela será uma lista vazia de intervalos. Aqui está um exemplo usando o AWS CLI para buscar a programação de largura de banda de um gateway:

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

Para editar a programação do controle de utilização de largura de banda de um gateway, use a ação `PutBandwidthRateLimitSchedule`. Observe que só é possível atualizar a programação de um gateway como um todo, em vez de modificar, adicionar ou remover intervalos individuais. Chamar essa ação substituirá a programação do controle de utilização de largura de banda anterior do gateway.

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

Trabalhar com hipervisores

Depois de terminarCriar um gateway, você pode conectá-lo a um hipervisor AWS Backup para permitir o trabalho com as máquinas virtuais gerenciadas por esse hipervisor. Por exemplo, o hipervisor para VMs da VMware é o VMware vCenter Server. Certifique-se de que o hipervisor esteja configurado com as permissões necessárias para o AWS Backup.

Adicionar um hipervisor

Como adicionar um hipervisor:

1. No painel de navegação esquerdo, na seção Recursos externos, escolha Hipervisores.
2. Escolha Adicionar hipervisor.
3. Na seção Configurações do hipervisor, digite o nome do hipervisor.
4. Para o host do vCenter Server, use o menu suspenso para selecionar o endereço IP ou o FQDN (nome de domínio totalmente qualificado). Digite o valor correspondente.
5. Para permitir AWS Backup a descoberta das máquinas virtuais no hipervisor, digite o nome de usuário e a senha do hipervisor.
6. Criptografe sua senha. Você pode especificar essa criptografia selecionando uma chave do KMS gerenciada pelo serviço específica ou uma chave do KMS gerenciada pelo cliente usando o menu suspenso ou escolhendo Criar chave do KMS. Se você não selecionar uma chave específica, o AWS Backup criptografará a senha usando uma chave de propriedade do serviço.
7. Na seção Conectar gateway, use a lista suspensa para especificar qual gateway conectar ao hipervisor.
8. Escolha Testar conexão de gateway para verificar as entradas anteriores.
9. Opcionalmente, na seção Tags do hipervisor, é possível atribuir tags ao hipervisor escolhendo Adicionar nova tag.
10. Mapeamento de tags VMware opcional: você pode adicionar até 10 tags VMware que você usa atualmente em suas máquinas virtuais para gerar tags. AWS
11. No painel de configuração do grupo de registros, você pode escolher a integração com o Amazon CloudWatch Logs para manter os registros do seu hipervisor (CloudWatch os preços padrão do Logs serão aplicados com base no uso). Cada hipervisor pode pertencer a um grupo de logs.

    a. Se você ainda não criou um grupo de logs, selecione o botão de opção Criar um grupo de logs. O hipervisor que você estiver editando será associado a esse grupo de logs.

b. Se já tiver criado um grupo de logs para um hipervisor diferente, você poderá usar esse grupo de logs para o hipervisor. Selecione Usar um grupo de logs existente.

c. Se você não quiser CloudWatch registrar, selecione Desativar registro.

12. Escolha Adicionar hipervisor, que levará você à página de detalhes.

> **Tip**
>
> Você pode usar o Amazon CloudWatch Logs (consulte a etapa 11 acima) para obter informações sobre seu hipervisor, incluindo monitoramento de erros, conexão de rede entre o gateway e o hipervisor e informações de configuração de rede. Para obter informações sobre grupos de CloudWatch registros, consulte Como trabalhar com grupos de registros e fluxos de registros no Guia do CloudWatch usuário da Amazon.

Visualizar máquinas virtuais gerenciadas por um hipervisor

Como visualizar máquinas virtuais em um hipervisor:

1. No painel de navegação esquerdo, na seção Recursos externos, escolha Hipervisores.
2. Na seção Hipervisores, escolha um hipervisor pelo nome do hipervisor para acessar sua página de detalhes.
3. Na seção Resumo do hipervisor, escolha a guia Máquinas virtuais.
4. Na seção Máquinas virtuais conectadas, uma lista de máquinas virtuais será preenchida automaticamente.

Visualizar gateways conectados a um hipervisor

Como visualizar gateways conectados a um hipervisor:

1. Escolha a guia Gateways.
2. Na seção Gateways conectados, uma lista de gateways será preenchida automaticamente.

Conectar um hipervisor a gateways adicionais

Suas velocidades de backup e de restauração podem ser limitadas pela largura de banda da conexão entre o gateway e o hipervisor. É possível aumentar essas velocidades conectando um ou

mais gateways adicionais ao seu hipervisor. Você pode fazer isso na seção Gateways conectados da seguinte forma:

1. Selecione Conectar.
2. Selecione outro gateway do usando o menu suspenso. Como alternativa, selecione Criar gateway para criar um gateway.
3. Selecione Conectar.

Editar a configuração de um hipervisor

Se não usar o recurso Testar conexão do gateway, você poderá adicionar um hipervisor com um nome de usuário ou senha incorretos. Nesse caso, o status da conexão do hipervisor será sempre `Pending`. Como alternativa, você pode alternar o nome de usuário ou a senha para acessar seu hipervisor. Atualize essas informações usando o seguinte procedimento:

Como editar um hipervisor já adicionado:

1. No painel de navegação esquerdo, na seção Recursos externos, escolha Hipervisores.
2. Na seção Hipervisores, escolha um hipervisor pelo nome do hipervisor para acessar sua página de detalhes.
3. Selecione a opção Editar.
4. O painel superior chama-se Configurações do hipervisor.
    a. No host do vCenter Server, também é possível editar o FQDN (nome de domínio totalmente qualificado) ou o endereço IP.
    b. Opcionalmente, insira o Nome de usuário e a Senha do hipervisor.
5. No painel de configuração do grupo de registros, você pode optar por se integrar à Amazon CloudWatch para manter os registros do seu hipervisor (o CloudWatch preço padrão será aplicado com base no uso). Cada hipervisor pode pertencer a um grupo de logs.
    a. Se você ainda não criou um grupo de logs, selecione o botão de opção Criar um grupo de logs. O hipervisor que você estiver editando será associado a esse grupo de logs.
    b. Se já tiver criado um grupo de logs para um hipervisor diferente, você poderá usar esse grupo de logs para o hipervisor. Selecione Usar um grupo de logs existente.
    c. Se você não quiser CloudWatch registrar, selecione Desativar registro.

> **Tip**
>
> Você pode usar o Amazon CloudWatch Logs (consulte a etapa 5 acima) para obter informações sobre seu hipervisor, incluindo monitoramento de erros, conexão de rede entre o gateway e o hipervisor e informações de configuração da rede. Para obter informações sobre grupos de CloudWatch registros, consulte Como trabalhar com grupos de registros e fluxos de registros no Guia do CloudWatch usuário da Amazon.

Para atualizar um hipervisor programaticamente, use o comando da CLI update-hypervisor e a chamada de API. UpdateHypervisor

Excluir a configuração de um hipervisor

Se você precisar remover um hipervisor já adicionado, remova a configuração do hipervisor e adicione outra. Essa operação de remoção se aplica à configuração para se conectar ao hipervisor. Isso não exclui o hipervisor.

Como excluir a configuração para se conectar a um hipervisor já adicionado:

1. No painel de navegação esquerdo, na seção Recursos externos, escolha Hipervisores.
2. Na seção Hipervisores, escolha um hipervisor pelo nome do hipervisor para acessar sua página de detalhes.
3. Escolha Remover e, depois, escolha Remover hipervisor.
4. Opcional: substitua a configuração do hipervisor removida usando o procedimento paraAdicionar um hipervisor.

Noções básicas sobre o status do hipervisor

A seguir, descrevemos cada um dos possíveis status do hipervisor e, se aplicável, as etapas de correção. O status `ONLINE` é o status normal do hipervisor. Um hipervisor deve ter esse status durante todo o tempo ou na maior parte do tempo em que estiver em uso para backup e recuperação de VMs gerenciadas pelo hipervisor.

Status do hipervisor

Status	Significado e correção
`ONLINE`	Você adicionou um hipervisor AWS Backup, associou a ele um gateway e pode se conectar a esse gateway pela sua rede para realizar backup e recuperação de máquinas virtuais gerenciadas pelo hipervisor. Você pode realizar backups sob demanda e programados dessas máquinas virtuais a qualquer momento.
`PENDING`	Você adicionou um hipervisor a AWS Backup , mas: • Ele não está associado a nenhum gateway ou • Ele está associado a um ou mais gateways, mas todos esses gateways foram excluídos ou não estão ativos. Para alterar o status de um hipervisor de `PENDING` para `ONLINE`, crie um gateway e conecte seu hipervisor a esse gateway.
`OFFLINE`	Você adicionou um hipervisor AWS Backup e o associou a um gateway, mas o gateway não pode se conectar ao hipervisor pela sua rede. Para alterar o status de um hipervisor de `OFFLINE` para`ONLINE`, verifique se a configuração da rede está correta. Se o problema persistir, verifique se o endereço IP ou nome de domínio totalment e qualificado do hipervisor está correto. Se estiverem incorretos, adicione o hipervisor

Status	Significado e correção
	novamente usando as informações corretas e teste a conexão de seu gateway.
ERROR	Você adicionou um hipervisor AWS Backup e o associou a um gateway, mas o gateway não pode se comunicar com o hipervisor. Para alterar o status de um hipervisor de ERROR para ONLINE, verifique se o nome de usuário e a senha do hipervisor estão corretos. Se estiverem incorretos, edite a configuração do hipervisor.

Próximas etapas

Para fazer backup de máquinas virtuais em seu hipervisor, consulte Fazer backup de máquinas virtuais.

Fazer backup de máquinas virtuais

Depois de Adicionar um hipervisor, o gateway de backup listará automaticamente suas máquinas virtuais. É possível visualizar suas máquinas virtuais escolhendo Hipervisores ou Máquinas virtuais no painel de navegação esquerdo.

- Escolha Hipervisores para visualizar somente as máquinas virtuais gerenciadas por um hipervisor específico. Com essa visualização, você pode trabalhar com uma máquina virtual por vez.
- Escolha Máquinas virtuais para visualizar todas as máquinas virtuais em todos os hipervisores que você adicionou ao seu. Conta da AWS Com essa visualização, você pode trabalhar com algumas ou todas as máquinas virtuais em vários hipervisores.

Independentemente da visualização escolhida, para realizar uma operação de backup em uma máquina virtual específica, escolha o nome da VM para abrir a página de detalhes. A página de detalhes da VM é o ponto de partida para os procedimentos a seguir.

Criar um backup sob demanda de uma máquina virtual

Um backup sob demanda é um backup único e completo que você inicia manualmente. Você pode usar backups sob demanda para testar os recursos AWS Backup de backup e restauração do.

Como criar um backup sob demanda de uma máquina virtual:

1. Escolha Criar backup sob demanda.
2. Configure o backup sob demanda.
3. Escolha Criar backup sob demanda.
4. Verifique quando seu trabalho de backup tem o status `Completed`. No painel de navegação esquerdo, escolha Trabalhos.
5. Escolha o ID do trabalho de backup para visualizar as informações do trabalho de backup, como o tamanho do backup e o tempo decorrido entre a Data de criação e a Data de conclusão.

Backups incrementais de VM

As versões mais recentes da VMware contêm um recurso chamado Changed Block Tracking (CBT), que monitora os blocos de armazenamento das máquinas virtuais à medida que eles mudam ao longo do tempo. Quando você usa AWS Backup para fazer backup de uma máquina virtual, AWS Backup tenta usar os dados do CBT, se estiverem disponíveis. AWS Backup usa dados de CBT para acelerar o processo de backup; sem dados de CBT, as tarefas de backup geralmente são mais lentas e usam mais recursos do hipervisor. O backup ainda pode ser concluído com êxito mesmo quando os dados de CBT não são válidos ou não estão disponíveis. Por exemplo, os dados de CBT podem não ser válidos ou não estar disponíveis se a máquina virtual ou o host do ESXi sofrer um desligamento forçado.

Nas ocasiões em que os dados de CBT forem inválidos ou estiverem indisponíveis, o status do backup será `Successful` com uma mensagem. Nesses casos, a mensagem indicará que, na ausência de dados de CBT, AWS Backup usou seu próprio mecanismo proprietário de detecção de alterações para concluir o backup em vez dos dados de CBT da VMware. Os backups subsequentes tentarão usar novamente os dados de CBT e, na maioria dos casos, os dados de CBT serão válidos e estarão disponíveis. Se o problema persistir, consulte Solução de problemas da VMware para obter as etapas de correção.

Para que o CBT funcione corretamente, o seguinte deve ser válido:

- O host deve ser ESXi 4.0 ou posterior

- A VM proprietária dos discos deve ter a versão de hardware 7 ou posterior
- O CBT deve estar habilitado para a máquina virtual (ele está habilitado por padrão)

Como verificar se um disco virtual tem o CBT habilitado:

1. Abra o vSphere Client e selecione uma máquina virtual desligada.
2. Clique com o botão direito do mouse na máquina virtual e navegue até Editar configurações > Opções > Avançado/Geral > Parâmetros de configuração.
3. A opção `ctkEnabled` deve ser igual a `True`.

Automatizar o backup de máquinas virtuais atribuindo recursos a um plano de backup

Um plano de backup é uma política de proteção de dados definida pelo usuário que automatiza a proteção de dados em vários serviços da AWS e aplicações de terceiros. Primeiro, você cria o plano de backup especificando sua frequência de backup, período de retenção, política de ciclo de vida e muitas outras opções. Para criar um plano de backup, consulte o tutorial de introdução.

Depois de criar seu plano de backup, você atribui recursos AWS Backup compatíveis, incluindo máquinas virtuais, a esse plano de backup. AWS Backup oferece várias maneiras de atribuir recursos, incluindo a atribuição de todos os recursos da sua conta, incluindo ou excluindo recursos específicos individuais ou a adição de recursos com determinadas tags.

Além dos recursos existentes de atribuição de recursos, o AWS Backup suporte para máquinas virtuais apresenta vários novos recursos para ajudá-lo a atribuir rapidamente máquinas virtuais aos planos de backup. Na página Máquinas virtuais, é possível atribuir tags a várias máquinas virtuais ou usar o novo recurso Atribuir recursos ao plano. Use esses recursos para atribuir suas máquinas virtuais já descobertas pelo AWS Backup gateway.

Se você prevê descobrir e atribuir máquinas virtuais adicionais no futuro e quiser automatizar a etapa de atribuição de recursos para incluir essas futuras máquinas virtuais, use o novo recurso Criar atribuição de grupo.

Etiquetas da VMware

Tags são pares chave/valor que ajudam você a gerenciar, filtrar e pesquisar seus recursos.

Uma tag da VMware é composta por uma categoria e um nome de tag. As tags da VMware são usadas para agrupar máquinas virtuais. Um nome de tag é um rótulo atribuído a uma máquina virtual. Uma categoria é uma coleção de nomes de tags.

Nas AWS tags, você pode usar caracteres entre letras UTF-8, números, espaços e caracteres especiais. `+ - = . _ : /`

Se usar tags em suas máquinas virtuais, você poderá adicionar até 10 tags correspondentes no AWS Backup para ajudar na organização. Você pode mapear até 10 tags VMware para AWS tags. No AWS Backup console, elas podem ser encontradas em Minha organização > Máquinas virtuais > AWS tags ou tags VMware.

Mapeamento de tags da VMware

Se usar tags em suas máquinas virtuais, você poderá adicionar até 10 tags correspondentes no AWS Backup para ajudar na organização. Os mapeamentos se aplicam a qualquer máquina virtual no hipervisor.

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No console, acesse Editar hipervisor (clique em Recursos externos, depois em Hipervisores, clique no nome do Hipervisor e clique em Gerenciar mapeamentos).
3. O último painel, mapeamento de tags da VMware, contém quatro campos de caixa de texto nos quais você pode inserir as informações existentes da tag VMware nas tags correspondentes. AWS Os quatro campos são categoria da tag Vmware, nome da tag VMware, chave da AWS tag e valor da AWS tag (exemplo: Categoria = OS; nome da tag = Windows; chave da AWS tag = OS-Windows e valor da AWS tag = Windows).
4. Depois de inserir seus valores preferidos, clique em Adicionar mapeamento. Se você cometer um erro, clique em Remover para excluir as informações inseridas.
5. Depois de adicionar os mapeamentos, especifique o perfil do IAM que você pretende usar para aplicar essas tags da AWS às máquinas virtuais da VMware.

   A política `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` contém as permissões necessárias. Você poderá anexar essa política ao perfil que estiver usando (ou fazer com que um administrador a anexe) ou criar uma política personalizada para o perfil que estiver sendo usado.
6. Por fim, clique em Adicionar hipervisor ou em Salvar.

A relação de confiança do perfil do IAM deve ser modificada para adicionar os serviços backup-gateway.amazonaws.com e backup.amazonaws.com. Sem esse serviços, você provavelmente receberá um erro ao mapear as tags. Para editar a relação de confiança para um perfil existente,

1. faça login no console do IAM.

2. No painel de navegação do console, selecione Perfis.
3. Escolha o nome do perfil que você deseja modificar e selecione a guia Relações de confiança na página de detalhes.
4. Em Documento da política, cole o seguinte:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "backup.amazonaws.com",
          "backup-gateway.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. Escolha Update Trust Policy.

Consulte Editar a relação de confiança de um perfil existente no Guia do administrador do AWS Directory Service para obter mais detalhes.

Exibir mapeamentos de tags da VMware

No console do AWS Backup, clique em Recursos externos, depois clique em Hipervisores e clique no link do nome do hipervisor para visualizar as propriedades do hipervisor selecionado. No painel de resumo, há quatro guias, a última das quais é Mapeamentos de tags da VMware. Observe que, se você ainda não tiver mapeamentos, “Não há mapeamentos de tags da VMware”. será exibido.

A partir daqui, você pode sincronizar os metadados das máquinas virtuais descobertas pelo hipervisor, copiar mapeamentos para seus hipervisores, adicionar AWS tags mapeadas às tags VMware à seleção de backup de um plano de backup ou gerenciar mapeamentos.

No console, para ver quais tags são aplicadas a uma máquina virtual selecionada, clique em Máquinas virtuais, depois no nome da máquina virtual e em Tags da AWS ou em Tags da VMware. É possível visualizar as tags associadas a essa máquina virtual e, também, gerenciar as tags.

Atribua máquinas virtuais ao plano usando mapeamentos de tags da VMware

Para atribuir máquinas virtuais a um plano de backup usando tags mapeadas, faça o seguinte:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No console, acesse Mapeamentos de tags da VMware na página de detalhes do hipervisor (clique em Recursos externos, depois em Hipervisores, e clique no nome do hipervisor).
3. Marque a caixa de seleção ao lado de várias tags mapeadas para atribuir essas tags ao mesmo plano de backup.
4. Clique em Adicionar à atribuição de recursos.
5. Escolha um Plano de backup existente na lista suspensa. Como alternativa, você pode escolher Criar um plano de backup, para criar um plano de backup.
6. Clique em Confirmar. Isso abrirá a página Atribuir recursos com os campos de Refinar seleção usando tags com os valores pré-preenchidos.

Tags da VMware usando o AWS CLI

AWS Backup usa a chamada de API `PutHypervisorPropertyMappings`para mapear as propriedades da entidade do hipervisor no local para as propriedades em. AWS

No AWS CLI, use a operação`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
```

Exemplo:

```
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
```

Também é possível usar GetHypervisorPropertyMappings para ajudar com informações de mapeamento de propriedades. No AWS CLI, use a operaçãoget-hypervisor-property-mappings. Veja um exemplo de modelo:

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

Exemplo:

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Sincronize metadados de máquinas virtuais descobertas pelo hipervisor AWS usando API, CLI ou SDK

É possível sincronizar os metadados das máquinas virtuais. Ao fazer isso, as tags da VMware presentes na máquina virtual que fazem parte dos mapeamentos serão sincronizadas. Além disso, as tags da AWS mapeadas para as tags da VMware presentes na máquina virtual serão aplicadas ao recurso de Máquina virtual da AWS .

AWS Backup usa a chamada de API StartVirtualMachinesMetadataSyncpara sincronizar os metadados das máquinas virtuais descobertas pelo hipervisor. Para sincronizar os metadados das máquinas virtuais descobertas pelo hipervisor usando a AWS CLI, use a operação start-virtual-machines-metadata-sync.

Exemplo de modelo:

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Exemplo:

```
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
```

Também é possível usar `GetHypervisor` para auxiliar com informações do hipervisor, como o host, o estado, o status da última sincronização de metadados e também para recuperar a hora da última sincronização de metadados bem-sucedida. No AWS CLI, use a operação`get-hypervisor`.

Exemplo de modelo:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Exemplo:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Para obter mais informações, consulte a documentação da API VmwareTag VmwareToAwsTagMappinge.

Esse recurso foi disponibilizado em novos gateways implantados após 15 de dezembro de 2022. Para os gateways existentes, esse novo recurso foi disponibilizado por meio de uma atualização automática de software em 30 de janeiro de 2023 ou antes dessa data. Para atualizar o gateway para a versão mais recente manualmente, use o AWS CLI comando UpdateGatewaySoftwareNow.

Exemplo:

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

Atribuir máquinas virtuais usando tags

Você pode atribuir suas máquinas virtuais atualmente descobertas por AWS Backup, junto com outros AWS Backup recursos, atribuindo a elas uma tag que você já atribuiu a um dos seus planos de backup existentes. Também é possível criar um plano de backup e uma atribuição de recursos com base em tags. Os planos de backup verificam os recursos recém-atribuídos sempre que executam um trabalho de backup.

Como marcar várias máquinas virtuais com a mesma tag:

1. No painel de navegação esquerdo, selecione Máquinas virtuais.

2. Marque a caixa de seleção ao lado do nome da VM para escolher todas as suas máquinas virtuais. Como alternativa, marque a caixa de seleção ao lado dos nomes das VMs que você deseja marcar.
3. Selecione Adicionar tags.
4. Digite uma chave de tag.
5. Recomendado: digite um valor de tag.
6. Selecione a opção Confirmar.

Atribuir máquinas virtuais usando o recurso Atribuir recursos ao plano

Você pode atribuir máquinas virtuais atualmente descobertas por AWS Backup a um plano de backup novo ou existente usando o recurso Atribuir recursos ao plano.

Como atribuir máquinas virtuais usando o recurso Atribuir recursos ao plano:

1. No painel de navegação esquerdo, selecione Máquinas virtuais.
2. Marque a caixa de seleção ao lado do nome da VM para escolher todas as suas máquinas virtuais. Como alternativa, marque a caixa de seleção ao lado de vários nomes de VM para atribuí-las ao mesmo plano de backup.
3. Escolha Atribuições e, depois, escolha Atribuir recursos ao plano.
4. Digite um nome de atribuição de recurso.
5. Escolha um Perfil do IAM de atribuição de recursos para criar backups e gerenciar pontos de recuperação. Se você não tiver um perfil do IAM específico para usar, recomendamos o perfil padrão, que tem as permissões corretas.
6. Na seção Plano de backup, escolha um plano de backup existente na lista suspensa. Como alternativa, escolha Criar plano de backup, para criar um plano de backup.
7. Escolha Atribuir recursos.
8. Opcional: verifique se as suas máquinas virtuais estão atribuídas a um plano de backup escolhendo Visualizar plano de backup. Depois, na seção Atribuições de recursos, escolha o Nome da atribuição de recurso.

Atribuir máquinas virtuais usando o recurso Criar atribuição de grupo

Diferentemente dos dois recursos de atribuição de recursos anteriores para máquinas virtuais, o recurso Criar atribuição de grupo não apenas atribui máquinas virtuais atualmente descobertas por

AWS Backup, mas também máquinas virtuais descobertas no futuro em uma pasta ou hipervisor definido por você.

Além disso, não é necessário marcar nenhuma caixa de seleção para usar o recurso Criar atribuição de grupo.

Como atribuir máquinas virtuais usando o recurso Atribuir recursos ao plano:

1. No painel de navegação esquerdo, selecione Máquinas virtuais.
2. Escolha Atribuições e, depois, escolha Criar atribuição de grupo.
3. Digite um nome de atribuição de recurso.
4. Escolha um Perfil do IAM de atribuição de recursos para criar backups e gerenciar pontos de recuperação. Se você não tiver um perfil do IAM específico para usar, recomendamos o perfil padrão, que tem as permissões corretas.
5. Na seção Grupo de recursos, selecione o menu suspenso Tipo de grupo. Suas opções são Pasta ou Hipervisor.

    a. Escolha Pasta para atribuir todas as máquinas virtuais em uma pasta em um hipervisor. Selecione um nome de grupo de pasta, como `datacenter/vm`, usando o menu suspenso. Também é possível optar por incluir Subpastas.

    > **Note**
    >
    > Para fazer atribuições baseadas em pastas, durante o processo de descoberta, AWS Backup marca as máquinas virtuais com a pasta em que elas são encontradas durante o processo de descoberta. Se você mover posteriormente uma máquina virtual para uma pasta diferente, AWS Backup não poderá atualizar a tag para você devido às práticas recomendadas de AWS marcação. Esse método de atribuição pode resultar na continuidade dos backups das máquinas virtuais que você retirou da pasta atribuída.

    b. Escolha Hipervisor para atribuir todas as máquinas virtuais gerenciadas por um hipervisor. Selecione um nome de grupo de ID do hipervisor usando o menu suspenso.
6. Na seção Plano de backup, escolha um plano de backup existente na lista suspensa. Como alternativa, escolha Criar plano de backup, para criar um plano de backup.
7. Escolha Criar atribuição de grupo.

8. Opcional: verifique se as suas máquinas virtuais estão atribuídas a um plano de backup escolhendo Visualizar plano de backup. Depois, na seção Atribuições de recursos, escolha o Nome da atribuição de recurso.

Próximas etapas

Para restaurar uma máquina virtual, consulte Restaurando uma máquina virtual usando AWS Backup.

Informações sobre componentes de origem de terceiros para o gateway de backup

Nesta seção, você pode encontrar informações sobre ferramentas e licenças de terceiros das quais dependemos para oferecer a funcionalidade de gateway de Backup.

O código-fonte de determinados componentes de software de origem incluídos com o software do gateway de backup está disponível para download nos seguintes locais:

- Para gateways implantados no VMware ESXi, faça download de sources.tzg.

Este produto inclui software desenvolvido pelo projeto OpenSSL para uso no OpenSSL Toolkit (https://www.openssl.org/).

Esse produto inclui software desenvolvido pelo VMware® vSphere Software Development Kit (https://www.vmware.com).

Para obter as licenças relevantes para todas as ferramentas de terceiros dependentes, consulte Licenças de terceiros.

Componentes de código aberto para o AWS Appliance

Várias ferramentas e licenças de terceiros são usadas para fornecer funcionalidade para o gateway de backup.

Use os links a seguir para baixar o código-fonte de determinados componentes de software de código aberto incluídos no software AWS Appliance:

- Para gateways implantados no VMware ESXi, faça download de sources.tar

Este produto inclui software desenvolvido pelo projeto OpenSSL para uso no OpenSSL Toolkit (https://www.openssl.org/). Para obter as licenças relevantes para todas as ferramentas de terceiros dependentes, consulte Licenças de terceiros.

Solução de problemas da VM

Backups incrementais/problemas e mensagens de CBT

Mensagem de falha: **"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."**

Se essa mensagem continuar, redefina o CBT conforme indicado pela VMware.

A mensagem observa que o CBT não estava ativado ou não estava disponível: “O VMware Change Block Tracking (CBT) não estava disponível para essa máquina virtual, mas o backup incremental foi concluído com êxito com nosso mecanismo de alteração proprietário”.

Verifique se o CBT está ativado. Como verificar se um disco virtual tem o CBT habilitado:

1. Abra o vSphere Client e selecione uma máquina virtual desligada.
2. Clique com o botão direito do mouse na máquina virtual e navegue até Editar configurações > Opções > Avançado/Geral > Parâmetros de configuração.
3. A opção `ctkEnabled` deve ser igual a `True`.

Se estiver ativado, verifique se você está usando os recursos do up-to-date VMware. O host deve ser o ESXi 4.0 ou posterior e a máquina virtual proprietária dos discos a serem rastreados deve ser da versão de hardware 7 ou posterior.

Se o CBT estiver ativado (habilitado) e o software e o hardware estiverem atualizados, desative a máquina virtual e ative-a novamente. Certifique-se de que o CBT esteja habilitado. Em seguida, execute o backup novamente.

Backup avançado do DynamoDB

AWS Backup oferece suporte a recursos adicionais e avançados para suas necessidades de proteção de dados do Amazon DynamoDB. Depois AWS Backup de ativar os recursos avançados no seu Região da AWS, você desbloqueia os seguintes recursos para todos os novos backups de tabela do DynamoDB que você criar:

- Economia e otimização de custos:
  - Hierarquização dos backups para o armazenamento frio para reduzir os custos de armazenamento
  - Marcação de alocação de custos para uso com o Cost Explorer
- Continuidade dos negócios:
  - Cópia entre regiões
  - Cópia entre contas
- Segurança:
  - Armazene backups em cofres do AWS Backup criptografados, que você pode proteger com o AWS Backup Vault Lock, políticas do AWS Backup e chaves de criptografia.
  - Os backups herdam tags de suas tabelas de origem do DynamoDB, permitindo que você use essas tags para definir permissões e políticas de controle de serviços (SCPs).

Os novos clientes que se inscreverem AWS Backup após novembro de 2021 terão os recursos avançados de backup do DynamoDB habilitados por padrão. Especificamente, os recursos avançados de backup do DynamoDB estão habilitados por padrão para clientes que não criaram um cofre de backup antes de 21 de novembro de 2021.

Recomendamos que todos os AWS Backup clientes existentes habilitem recursos avançados para o DynamoDB. Não há diferença no preço do armazenamento de backup quente depois que os recursos avançados forem habilitados. Você pode economizar dinheiro hierarquizando os backups para o armazenamento frio e otimizando seus custos usando tags de alocação de custos. Você também pode começar a aproveitar os recursos AWS Backup de continuidade de negócios e segurança da.

> **Note**
>
> Se você usar uma função ou política personalizada em vez AWS Backup da função de serviço padrão, deverá adicionar ou usar as seguintes políticas de permissões (ou adicionar as permissões equivalentes) à sua função personalizada:
>
> - `AWSBackupServiceRolePolicyForBackup` para realizar backup avançado do DynamoDB.
> - `AWSBackupServiceRolePolicyForRestores` para restaurar backups avançados do DynamoDB.

Para saber mais sobre políticas AWS gerenciadas e ver exemplos de políticas gerenciadas pelo cliente, consulte. Políticas gerenciadas para AWS Backup

Tópicos

Habilitar o backup avançado do DynamoDB usando o console

Você pode ativar recursos AWS Backup avançados para backups do DynamoDB usando o console do DynamoDB AWS Backup ou do DynamoDB.

Para ativar os recursos avançados de backup do DynamoDB a partir do console: AWS Backup

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No menu de navegação esquerdo, selecione Configurações.
3. Na seção Serviços compatíveis, verifique se o DynamoDB está habilitado.

   Se não estiver, escolha Ingressar e habilite o DynamoDB como um serviço compatível com o AWS Backup .
4. Na seção Recursos avançados para backups do DynamoDB, escolha Habilitar.
5. Escolha Habilitar recursos.

Para saber como habilitar recursos AWS Backup avançados usando o console do DynamoDB, consulte AWS Backup Habilitando recursos no Guia do usuário do Amazon DynamoDB.

Habilitar o backup avançado do DynamoDB de forma programática

Você também pode ativar recursos AWS Backup avançados para backups do DynamoDB usando a AWS Command Line Interface (CLI). Você habilita os backups avançados do DynamoDB ao definir os dois valores a seguir como `true`:

Para habilitar programaticamente recursos AWS Backup avançados para backups do DynamoDB:

1. Verifique se você já habilitou os recursos AWS Backup avançados para o DynamoDB usando o seguinte comando:

   ```
   $ aws backup describe-region-settings
   ```

   Se estiver `"DynamoDB":true` em `"ResourceTypeManagementPreference"` e `"ResourceTypeOptInPreference"`, você já habilitou o backup avançado do DynamoDB.

   Se, como na saída a seguir, você tiver pelo menos uma instância de `"DynamoDB":false` e ainda não tiver habilitado o backup avançado do DynamoDB, prossiga para a próxima etapa.

   ```
   {
     "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. Use a operação `UpdateRegionSettings` a seguir para definir `"ResourceTypeManagementPreference"` e `"ResourceTypeOptInPreference"` como `"DynamoDB":true`:

```
aws backup update-region-settings \
              --resource-type-opt-in-preference DynamoDB=true \
              --resource-type-management-preference DynamoDB=true
```

Editar um backup avançado do DynamoDB

Ao criar um backup do DynamoDB depois de AWS Backup ativar os recursos avançados, você pode usar para: AWS Backup

- Copiar um backup entre regiões
- Copiar um backup entre contas
- Alterar quando AWS Backup hierarquiza um backup para armazenamento refrigerado
- Marcar o backup

Para usar esses recursos avançados em um backup existente, consulte Editar um backup.

Se você desabilitar posteriormente os recursos AWS Backup avançados do DynamoDB, poderá continuar executando essas operações nos backups do DynamoDB que você criou durante o período em que ativou os recursos avançados.

Restaurar um backup avançado do DynamoDB

Você pode restaurar os backups do DynamoDB feitos AWS Backup com os recursos avançados habilitados da mesma forma que restaura os backups do DynamoDB feitos antes de ativar os recursos avançados. AWS Backup Você pode realizar uma restauração usando um AWS Backup ou o DynamoDB.

Você pode especificar como criptografar sua tabela recém-restaurada com as seguintes opções:

- Ao restaurar na mesma região da tabela original, você pode, opcionalmente, especificar uma chave de criptografia para a tabela restaurada. Se você não especificar uma chave de criptografia, AWS Backup criptografará automaticamente sua tabela restaurada usando a mesma chave que criptografou sua tabela original.
- Ao restaurar em uma região diferente da tabela original, você deverá especificar uma chave de criptografia.

Para restaurar o uso AWS Backup, consulteRestaurar uma tabela do Amazon DynamoDB.

Para restaurar usando o DynamoDB, consulte Restaurar uma tabela do DynamoDB a partir de um backup no Guia do usuário do Amazon DynamoDB.

Excluir um backup avançado do DynamoDB

Não é possível excluir backups criados usando esses recursos avançados no DynamoDB. Você deve usar o AWS Backup para excluir backups para manter a consistência global em todo o seu ambiente da AWS .

Para excluir um backup do DynamoDB, consulte Excluir backups.

Outros benefícios do gerenciamento completo do AWS Backup quando você habilita o backup avançado do DynamoDB

Ao habilitar recursos AWS Backup avançados para o DynamoDB, você oferece gerenciamento completo dos seus backups do DynamoDB a. AWS Backup Isso fornece os seguintes benefícios adicionais:

Criptografia

AWS Backup criptografa automaticamente os backups com a chave KMS do seu cofre de destino AWS Backup . Anteriormente, eles eram criptografados usando o mesmo método de criptografia da tabela de origem do DynamoDB. Isso aumenta o número de defesas que você pode usar para proteger seus dados. Consulte Criptografia para backups em AWS Backup Para mais informações.

Nome do recurso da Amazon (ARN)

Cada namespace de serviço do ARN de backup é `awsbackup`. Anteriormente, o namespace do serviço era `dynamodb`. Em outras palavras, o início de cada ARN mudará de `arn:aws:dynamodb` para `arn:aws:backup`. Consulte ARNs for AWS Backup na Referência de autorização do serviço.

Com essa alteração, você ou seu administrador de backups podem criar políticas de acesso para os backups usando o namespace do serviço `awsbackup` que agora se aplica aos backups do DynamoDB criados após a habilitação dos recursos avançados. Ao usar o namespace do serviço `awsbackup`, também é possível aplicar políticas a outros backups feitos pelo AWS Backup. Consulte Controle de acesso Para mais informações.

Localização das cobranças no extrato de faturamento

As cobranças por backups (incluindo armazenamento, transferências de dados, restaurações e exclusão antecipada) aparecem em “Backup” na sua AWS fatura. Anteriormente, as cobranças apareciam em “DynamoDB” na fatura.

Essa alteração garante que você possa usar o AWS Backup faturamento para monitorar centralmente seus custos de backup. Consulte Medição, custos e cobrança Para mais informações.

Backups do Amazon Timestream

O Amazon Timestream é um banco de dados de séries temporais escalável que permite o armazenamento e a análise de até trilhões de pontos de dados de séries temporais diariamente. O Timestream é otimizado para economizar custos e tempo, mantendo os dados recentes na memória e armazenando dados históricos em um nível de armazenamento com custo otimizado, de acordo com suas políticas.

Um banco de dados do Timestream tem tabelas. Essas tabelas contêm registros e cada registro é um ponto de dados único em uma série temporal. Uma série temporal é uma sequência de registros registrados em um intervalo de tempo, como preço de ações, nível de uso da memória de uma instância do Amazon EC2 ou leitura de temperatura. AWS Backup pode fazer backup e restaurar centralmente tabelas de Timestream. Você pode copiar esses backups de tabela para outras contas e várias outras Regiões da AWS dentro da mesma organização.

Atualmente, o Timestream não oferece serviços nativos de backup e restauração, portanto, usar AWS Backup para criar cópias seguras de suas tabelas do Timestream pode adicionar uma camada extra de segurança e resiliência aos seus recursos.

Fazer backup de tabelas do Timestream

Você pode fazer backup das tabelas do Timestream por meio do AWS Backup console ou usando o. AWS CLI

Há duas maneiras de usar o AWS Backup console para fazer backup de uma tabela Timestream: sob demanda ou como parte de um plano de backup.

Criar backups sob demanda do Timestream

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Usando o painel de navegação, escolha Recursos protegidos e Criar backup sob demanda.
3. Na página Criar backup sob demanda, escolha Amazon Timestream.

4. Escolha Tipo de recurso Timestream e, em seguida, escolha o nome da tabela da qual você deseja fazer backup.
5. Verifique se a opção Criar backup agora está selecionada. Isso iniciará um backup imediatamente e permitirá que você veja seu cluster antes na página Recursos protegidos.
6. No menu suspenso Transição para armazenamento frio, defina as configurações de transição.
7. Em Período de retenção, é possível escolher por quanto tempo reter o backup.
8. Escolha um cofre de backup existente ou crie um. Ao escolher Criar cofre de backup uma nova página será aberta para criar um cofre e você será redirecionado para a página Criar backup sob demanda ao concluir.
9. Em Função do IAM, escolha Função AWS Backup padrão (se a função padrão não estiver presente na sua conta, ela será criada para você com as permissões corretas).
10. Opcionalmente, as tags podem ser adicionadas ao seu ponto de recuperação. Se você deseja atribuir uma ou mais tags ao seu backup sob demanda, insira uma chave e um valor opcional, e escolha Adicionar tag.
11. Escolha Criar backup sob demanda. Dessa forma, você será redirecionado para a página Trabalhos, onde verá uma lista de trabalhos.
12. Escolha o ID do trabalho de backup para o cluster para ver os detalhes desse trabalho. Ele exibirá um status de`Completed`, `In Progress` ou `Failed`. Você pode clicar no ícone Atualizar para atualizar o status.

Criar backups programados do Timestream em um plano de backup

Seus backups programados podem incluir tabelas do Timestream se elas forem um recurso protegido. Como optar por proteger as tabelas do Amazon Timestream:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos.
3. Alterne o Amazon Timestream para Ativado.
4. Consulte Atribuição de recursos ao console para incluir tabelas do Timestream em um plano novo ou existente.

Em Gerenciar planos de backup, você pode optar por criar um plano de backup e incluir tabelas do Timestream, ou pode atualizar um existente para incluir tabelas do Timestream. Ao adicionar o tipo

de recurso Timestream, você pode optar por adicionar Todas as tabelas do Timestream ou marcar as caixas ao lado das tabelas que você deseja adicionar em Selecionar tipos de recursos específicos.

O primeiro backup feito das tabelas do Timestream será um backup completo. Os backups subsequentes serão backups incrementais.

Depois de criar ou modificar o plano de backup, navegue até Planos de backup no painel de navegação esquerdo. O plano de backup que você especificou deve exibir seus clusters em Atribuições de recursos.

Fazer backup de forma programática

Também é possível usar o nome de operação `start-backup-job`. Inclua os seguintes parâmetros:

```
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 Região da AWS \
--endpoint-url URL
```

Visualizar backups de tabela do Timestream

Como visualizar e modificar seus backups de tabela do Timestream no console:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Escolha Cofres de backup. Em seguida, clique no nome do cofre de backup que contém as tabelas do Timestream.
3. O cofre de backup exibirá um resumo e uma lista de backups.
    a. É possível clicar no link na coluna ID do ponto de recuperação ou
    b. você pode marcar a caixa à esquerda do ID do ponto de recuperação e clicar em Ações para excluir os pontos de recuperação que não sejam mais necessários.

Restaurar uma tabela do Timestream

Veja como restaurar uma tabela do Timestream

Backup de bancos de dados SAP HANA em instâncias do Amazon EC2

> **Note**
>
> Serviços suportados por Região da AWScontém as regiões atualmente suportadas nas quais os backups do banco de dados SAP HANA nas instâncias do Amazon EC2 estão disponíveis.

AWS Backup oferece suporte a backups e restaurações de bancos de dados SAP HANA em instâncias do Amazon EC2.

Tópicos

Visão geral dos bancos de dados SAP HANA com AWS Backup

Além da capacidade de criar backups e restaurar bancos de dados, a integração do AWS Backup com o Amazon EC2 Systems Manager para SAP permite que os clientes identifiquem e marquem bancos de dados SAP HANA.

AWS Backup é integrado ao AWS Backint Agent para realizar backups e restaurações do SAP HANA. Para obter mais informações, consulte AWS Backint.

Pré-requisitos para fazer backup de bancos de dados SAP HANA por meio de AWS Backup

Vários pré-requisitos devem ser preenchidos antes que as atividades de backup e restauração possam ser executadas. Observe que você precisará de acesso administrativo ao seu banco de

dados e permissões do SAP HANA para criar novas funções e políticas do IAM em sua AWS conta para realizar essas etapas.

Preencha esses pré-requisitos no Amazon EC2 Systems Manager.

1. Configure as permissões necessárias para a instância do Amazon EC2 executando o banco de dados SAP HANA
2. Registre as credenciais em AWS Secrets Manager
3. Instale o AWS Backint e AWS Systems Manager para agentes SAP
4. Verifique o SSM Agent
5. Verifique os parâmetros
6. Registre o banco de dados SAP HANA

É uma prática recomendada registrar cada instância do HANA apenas uma vez. Vários registros podem resultar em vários ARNs para o mesmo banco de dados. A manutenção de um único ARN e registro simplifica a criação e a manutenção do plano de backup e também pode ajudar a reduzir a duplicação não planejada de backups.

Operações de backup do SAP HANA no console AWS Backup

Depois que os pré-requisitos e o SSM para as configurações do SAP estiverem preenchidos, você poderá fazer backup e restaurar seu SAP HANA em bancos de dados do EC2.

Optar por proteger os recursos do SAP HANA

Para ser usado AWS Backup para proteger seus bancos de dados SAP HANA, o SAP HANA deve ser ativado como um dos recursos protegidos. Para fazer a inclusão:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Configurações.
3. Em Optar pela adoção do serviço, selecione Configurar recursos.
4. Opte por incluir o SAP HANA no Amazon EC2.
5. Clique em Confirmar.

A inclusão do serviço SAP HANA no Amazon EC2 agora será habilitada.

Crie um backup programado dos bancos de dados SAP HANA

É possível editar um plano de backup existente e adicionar recursos do SAP HANA a ele, ou criar um plano de backup apenas para os recursos do SAP HANA.

Se optar por criar um plano de backup, você terá três opções:

1. Opção 1: começar com um modelo
    1. Escolha um modelo de plano de backup.
    2. Especifique um nome de plano de backup.
    3. Clique em Criar plano.
2. Opção 2: criar um plano
    1. Especifique um nome de plano de backup.
    2. Opcionalmente, especifique as tags a serem adicionadas ao plano de backup.
    3. Especifique a configuração da regra de backup.
        a. Especifique um nome de regra de backup.
        b. Escolha um cofre existente ou crie um. Este é o local em que seus backups serão armazenados.
        c. Especifique uma frequência de backup.
        d. Especifique uma janela de backup.

            Observe que a transição para o armazenamento frio não é compatível no momento.
        e. Especifique o período de retenção.

            No momento, a cópia para o destino não é compatível
        f. (Opcional) Especifique as tags a serem adicionadas aos pontos de recuperação.
    4. Clique em Criar plano.
3. Opção 3: definir um plano usando JSON
    1. Especifique o JSON para seu plano de backup modificando a expressão JSON de um plano de backup existente ou criando uma expressão.
    2. Especifique um nome de plano de backup.
    3. Clique em Validar JSON.

Depois que o plano de backup for criado com êxito, você poderá atribuir recursos ao plano de backup na próxima etapa.

Seja qual for o plano usado, assegure-se de atribuir recursos. É possível escolher quais bancos de dados SAP HANA atribuir, incluindo bancos de dados do sistema e do locatário. Você também tem a opção de excluir IDs de recursos específicos.

Crie um backup sob demanda dos bancos de dados SAP HANA

É possível criar um backup completo sob demanda que seja executado imediatamente após a criação. Observe que os backups sob demanda de bancos de dados SAP HANA em instâncias do Amazon EC2 são backups completos. Os backups incrementais não são compatíveis.

Seu backup sob demanda foi criado. Ele começará a fazer backup dos recursos especificados. O console fará a transição para a página Trabalhos de backup, na qual você poderá ver o progresso do trabalho. Anote o ID do trabalho de backup no banner azul na parte superior da tela, pois você precisará dele para encontrar facilmente o status do trabalho de backup. Quando o backup for concluído, o status progredirá para `Completed`. Os backups podem levar várias horas.

Atualize a Lista de trabalho de backup para ver a alteração do status. Você também pode pesquisar e clicar no ID do trabalho de backup para ver o status detalhado do trabalho.

Backups contínuos dos bancos de dados SAP HANA

Você pode fazer backups contínuos, que podem ser usados com point-in-time restauração (PITR) (observe que os backups sob demanda preservam os recursos no estado em que são usados; enquanto o PITR usa backups contínuos que registram as alterações durante um período de tempo).

Com backups contínuos, é possível restaurar seu banco de dados do SAP HANA em uma instância do EC2 retornando-o para um horário específico de sua escolha, com precisão de 1 segundo (retrocesso máximo de 35 dias). O backup contínuo funciona criando primeiramente um backup completo do seu recurso e, em seguida, fazendo backup constante dos logs de transações do recurso. A restauração da PITR funciona acessando seu backup completo e reproduzindo o registro de transações até o momento em que você solicita AWS Backup a recuperação.

Você pode optar por backups contínuos ao criar um plano de backup AWS Backup usando o AWS Backup console ou a API.

Como habilitar os backups contínuos usando o console

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Planos de backup e, depois, escolha Criar plano.
3. Em Regras de backup, escolha Adicionar regra de backup.
4. Na seção Configuração da regra de backup, selecione Habilitar backups contínuos para recursos compatíveis.

Depois de desativar a PITR (point-in-timerestauração) para backups do banco de dados SAP HANA, os registros continuarão sendo enviados AWS Backup até que o ponto de recuperação expire (status igual a). `EXPIRED`) É possível mudar para um local alternativo de backup de logs no SAP HANA para interromper a transmissão de logs para o AWS Backup.

Um ponto de recuperação contínuo com um status de `STOPPED` indica que um ponto de recuperação contínuo foi interrompido; ou seja, os registros transmitidos do SAP HANA para AWS Backup aquele mostram que as alterações incrementais em um banco de dados têm uma lacuna. Os pontos de recuperação que ocorrerem dentro desse intervalo de tempo terão um status de `STOPPED`..

Para problemas que você possa encontrar durante os trabalhos restauração de backups contínuos (pontos de recuperação), consulte a seção de Solução de problemas de restauração do SAP HANA deste guia.

Veja os backups do banco de dados SAP HANA

Visualize o status dos trabalhos de backup:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Trabalhos.
3. Escolha os trabalhos de backup, trabalhos de restauração ou trabalhos de cópia para ver a lista de seus trabalhos.
4. Pesquise e clique no ID do trabalho de backup para ver os status detalhados do trabalho.

Visualize todos os pontos de recuperação em um cofre:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Cofres de backup.

3. Pesquise e clique em um cofre de backup para visualizar todos os pontos de recuperação no cofre.

Visualize detalhes dos recursos protegidos:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos.
3. Você também pode filtrar por tipo de recurso para visualizar todos os backups desse tipo de recurso.

Use AWS CLI para bancos de dados SAP HANA com AWS Backup

Cada ação no console do Backup tem uma chamada de API correspondente.

Para configurar AWS Backup e gerenciar programaticamente seus recursos, use a chamada de API `StartBackupJob`para fazer backup de um banco de dados SAP HANA em uma instância do EC2.

Use o comando `start-backup-job` da CLI.

Solução de problemas de backups de bancos de dados SAP HANA

Se você encontrar erros durante o fluxo de trabalho, consulte os seguintes exemplos de erros e resoluções sugeridas:

Pré-requisitos do Python

- Erro: erro do Zypper relacionado à versão do Python desde o SSM para SAP e requer o Python 3.6, mas o SUSE 12 SP5, por padrão, é compatível com o AWS Backup Python 3.4.

  Resolução: instale várias versões do Python no SUSE12 SP5 seguindo as seguintes etapas:

  1. Execute um comando update-alternatives para criar um link simbólico para o Python 3 em '/usr/local/bin/' em vez de usar diretamente '/usr/bin/python3'. Esses comandos definirão o Python 3.4 como a versão padrão. O comando é: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.4 5`
  2. Adicione o Python 3.6 à configuração de alternativas executando o seguinte comando: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`

3. Altere a configuração alternativa para o Python 3.6 executando o seguinte comando: `# sudo update-alternatives –config python3`

   A seguinte saída deve ser exibida:

   ```
   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. Digite o número correspondente ao Python 3.6.
5. Verifique a versão do Python e confirme se o Python 3.6 está sendo usado.
6. (Opcional, mas recomendado) Verifique se os comandos do Zypper funcionam conforme o esperado.

Amazon EC2 Systems Manager para descoberta e registro de SAP

- Erro: o SSM para SAP falhou ao descobrir a carga de trabalho devido ao bloqueio do acesso ao endpoint público e ao SSM. AWS Secrets Manager

  Resolução: teste se os endpoints podem ser acessados a partir do seu banco de dados SAP HANA. Se eles não puderem ser alcançados, você pode criar endpoints Amazon VPC AWS Secrets Manager e SSM para SAP.

  1. Teste o acesso ao Secrets Manager do host Amazon EC2 para HANA DB executando o seguinte comando:. `aws secretsmanager get-secret-value –secret-id hanaeccsbx_hbx_database_awsbkp` Se o comando não retornar um valor, o firewall está bloqueando o acesso ao endpoint do serviço Secrets Manager. O registro será interrompido na etapa “Recuperando segredos do Secrets Manager”.
  2. Teste a conectividade com o SSM para o endpoint SAP executando o comando. `aws ssm-sap list-registration` Se o comando não retornar um valor, o firewall está bloqueando o acesso ao SSM para o endpoint SAP.

     Exemplo de erro:`Connection was closed before we received a valid response from endpoint URL: “https://ssm-sap.us-west-2.amazonaws.com/register-application"`.

Há duas opções para continuar se os endpoints não estiverem acessíveis.

- Abra portas de firewall para permitir acesso ao endpoint de serviço público para Secrets Manager e SSM for SAP; ou,
- Crie endpoints VPC para Secrets Manager e SSM para SAP e, em seguida:
  - Certifique-se de que a Amazon VPC esteja habilitada para DNSSupport e DNSHostName.
  - Certifique-se de que seu VPC endpoint tenha ativado a opção Permitir nome DNS privado.
  - Se a descoberta do SSM para SAP for concluída com êxito, o log mostrará que o host foi descoberto.

- Erro: AWS Backup e a conexão do Backint falha devido ao bloqueio do acesso aos endpoints públicos do AWS Backup serviço. `aws-backint-agent.log`pode mostrar erros semelhantes a este: `time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id" oulevel=fatal msg="Error performing backup missing backup data plane Id`. Além disso, o AWS Backup console pode mostrar `Fatal Error: An internal error occured.`

  Resolução: Há duas opções para continuar se os endpoints não estiverem acessíveis:

  - Abra portas de firewall para permitir o acesso aos endpoints de serviço público (HTTPS). Depois que essa opção for usada, o DNS resolverá as solicitações aos AWS serviços por meio de endereços IP públicos.
  - Crie endpoints de VPC e roteie de forma privada o tráfego de e para os serviços necessários para. AWS AWS Backup Depois que essa opção for usada, o DNS resolverá as solicitações desses serviços por meio de endereços IP privados. Essa opção pode exigir atualizações no servidor DNS para adicionar regras para encaminhar solicitações para endpoints privados.

- Erro: o SSM para registro do SAP falha devido à senha do HANA contendo caracteres especiais. Exemplos de erros podem incluir `Error connecting to database HBX/HBX when validating its credentials.` ou `Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated.` após testar uma conexão usando `hdbsql` for `systemdb` e `tenantdb` que foi testada a partir da instância Amazon EC2 do banco de dados HANA.

  No AWS Backup console da página Trabalhos, os detalhes do trabalho de backup podem mostrar o status `FAILED` com o erro`Miscellaneous: b’* 10: authentication failed SQLSTATE: 28000\n’`.

Resolução: Certifique-se de que sua senha não tenha caracteres especiais, como $.

- Erro: **`b'* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...`**

  Resolução: A instalação do AWS BackInt Agent for SAP HANA pode não ter sido concluída com êxito. Repita o processo para implantar o AWS Backint Agent e o Amazon EC2 Systems Manager Agent em seu servidor de aplicativos SAP.

- Erro: o console não corresponde aos arquivos de log após o registro.

  O registro de descoberta mostra falha no registro ao tentar se conectar ao HANA DB devido à senha contendo caracteres especiais, embora o console SSM para SAP Application Manager for SAP exiba o registro bem-sucedido. Ele não confirma que o registro foi bem-sucedido. Se o console mostrar um registro bem-sucedido, mas os registros não, os backups falharão.

  Confirme o status do registro:

  1. Faça login no console SSM
  2. Selecione Executar comando na navegação do lado esquerdo.
  3. No campo de texto Histórico do comando, insira`Instance ID:Equal:`, com o valor igual à instância que você usou para o registro. Isso filtrará o histórico de comandos.
  4. Use a coluna ID do comando para encontrar comandos com status`Failed`. Em seguida, encontre o nome do documento AWSSystemsManagerSAP-Discovery.
  5. No AWS CLI, execute o comando`aws ssm-sap register-application status`. Se o valor retornado for exibido`Error`, o registro não foi bem-sucedido.

  Resolução: Certifique-se de que sua senha do HANA não tenha caracteres especiais (como '$').

Criando um backup de um banco de dados SAP HANA

- Erro: o AWS Backup console exibe a mensagem “Erro fatal” quando um backup sob demanda para SystemDB ou TenantDB é criado. Isso ocorre porque o endpoint público cell-1.prod.us-west-2.storage.cryo.aws.a2z.com não pode ser acessado. Isso é causado por um firewall do lado do cliente que bloqueia o acesso a esse endpoint.

  `aws-backint-agent.log`pode mostrar erros como `level=error msg="Storage configuration validation failed: missing backup data plane Id"` ou `level=fatal msg="Error performing backup missing backup data plane Id."`

Resolução: acesso de firewall aberto ao endpoint público cell-1.prod.us-west-2.storage.cryo.aws.a2z.com.

- Erro:`Database cannot be backed up while it is stopped.`

  Resolução: certifique-se de que o banco de dados a ser copiado esteja ativo. Os dados e logs do banco de dados só poderão ser copiados enquanto o banco de dados estiver online.
- Erro: `Getting backup metadata failed. Check the SSM document execution for more details.`

  Resolução: certifique-se de que o banco de dados a ser copiado esteja ativo. Os dados e logs do banco de dados só poderão ser copiados enquanto o banco de dados estiver online.

Monitorando registros de backup

- Erro: `Encountered an issue with log backups, please check SAP HANA for details.`

  Resolução: verifique o SAP HANA para garantir que os backups de log estejam sendo enviados AWS Backup do SAP HANA.
- Erro: `One or more log backup attempts failed for recovery point.`

  Resolução: consulte o SAP HANA para obter detalhes. Certifique-se de que os backups de log estejam sendo enviados AWS Backup do SAP HANA.
- Erro: `Unable to determine the status of log backups for recovery point.`

  Resolução: consulte o SAP HANA para obter detalhes. Certifique-se de que os backups de log estejam sendo enviados AWS Backup do SAP HANA.
- Erro: `Log backups for recovery point %s were interrupted due to a restore operation on the database.`

  Resolução: aguarde a conclusão do trabalho de restauração. Os backups de logs devem ser retomados.

Glossário de termos do SAP HANA ao usar AWS Backup

Tipos de backup de dados: O SAP HANA suporta dois tipos de backups de dados: completo e INC (incremental). AWS Backup otimiza qual tipo é usado durante cada operação de backup.

Backups de catálogos: o SAP HANA mantém seu próprio manifesto chamado catálogo. AWS Backup interage com esse catálogo. Cada novo backup criará uma entrada no catálogo.

Backup contínuo de logs (logs de transações): para funções de recuperação para um ponto no tempo (PITR), o SAP HANA rastreia todas as transações desde o backup mais recente.

Cópia do sistema: um trabalho de restauração no qual o banco de dados de destino da restauração é diferente do banco de dados de origem a partir do qual o ponto de recuperação foi criado.

Restauração destrutiva: uma restauração destrutiva é um tipo de trabalho de restauração durante o qual um banco de dados restaurado exclui ou substitui o banco de dados de origem ou existente.

COMPLETO: um backup completo é um backup de um banco de dados completo.

INC: Um backup incremental é um backup de todas as alterações em um banco de dados SAP HANA desde o backup anterior.

Para obter detalhes adicionais, consulte o glossário da AWS.

AWS Backup suporte de bancos de dados SAP HANA em instâncias EC2

Algumas funcionalidades não são compatíveis no momento:

- No momento, a cópia entre contas e entre regiões não são compatíveis.
- No momento o Backup Audit Manager e os relatórios não são compatíveis.
- Serviços suportados por Região da AWScontém as regiões atualmente suportadas para backups de bancos de dados SAP HANA em instâncias do Amazon EC2.

Backups do Amazon Redshift

O Amazon Redshift é um data warehouse em nuvem totalmente gerenciado e escalável que acelera seu tempo de obtenção de insights com análises rápidas, fáceis e seguras. Você pode usar AWS Backup para proteger seus data warehouses com backups imutáveis, políticas de acesso separadas e governança organizacional centralizada das tarefas de backup e restauração.

Um data warehouse do Amazon Redshift é uma coleção de recursos computacionais chamados nós, que são organizados em um grupo chamado cluster. AWS Backup pode fazer backup desses clusters.

Para obter informações sobre o Amazon Redshift, consulte o Guia de introdução ao Amazon Redshift o Guia do desenvolvedor de banco de dados do Amazon Redshift e o Guia de gerenciamento de clusters do Amazon Redshift.

Fazer backup de clusters provisionados do Amazon Redshift

Você pode proteger seus clusters do Amazon Redshift usando o AWS Backup console ou programaticamente usando API ou CLI. O backup desses clusters pode ser feito regularmente como parte de um plano de backup ou podem ser feito conforme necessário por meio do backup sob demanda.

É possível restaurar uma única tabela (também conhecida como restauração em nível de item) ou um cluster inteiro. Observe que não é possível fazer o backup somente das tabelas. O backup das tabelas é feito como parte de um cluster quando o backup dele é feito.

AWS Backup O uso permite que você visualize seus recursos de forma centralizada; no entanto, se o Amazon Redshift for o único recurso que você usa, você pode continuar usando o agendador automático de snapshots no Amazon Redshift. Observe que você não pode continuar gerenciando as configurações manuais de snapshots usando o Amazon Redshift se optar por gerenciá-las via. AWS Backup

Você pode fazer backup dos clusters do Amazon Redshift por meio do AWS Backup console ou usando o. AWS CLI

Há duas maneiras de usar o AWS Backup console para fazer backup de um cluster do Amazon Redshift: sob demanda ou como parte de um plano de backup.

Criar backups sob demanda do Amazon Redshift

Consulte a página Criar um tipo de backup sob demanda para obter mais informações.

Para criar um snapshot manual, deixe a caixa de seleção de backup contínuo desmarcada ao criar um plano de backup que inclua recursos do Amazon Redshift.

Criar backups programados do Amazon Redshift em um plano de backup

Seus backups programados podem incluir clusters do Amazon Redshift se eles forem um recurso protegido. Como optar por proteger as tabelas do Amazon Redshift:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.

2. No painel de navegação, escolha Recursos protegidos.
3. Alterne o Amazon Redshift para Ativado.
4. Consulte Atribuir recursos ao console para incluir clusters do Amazon Redshift em um plano novo ou existente.

Em Gerenciar planos de backup, você pode optar por criar um plano de backup e incluir clusters do Amazon Redshift, ou pode atualizar um existente para incluir clusters do Amazon Redshift. Ao adicionar o tipo de recurso Amazon Redshift, você pode optar por adicionar Todos os clusters do Amazon Redshift ou marcar as caixas ao lado dos clusters que você

faz backup de forma programática

Você também pode definir seu plano de backup em um documento JSON e fornecê-lo usando o AWS Backup console ou AWS CLI. Consulte Criação de planos de backup usando um documento JSON e a AWS Backup CLI para obter informações sobre como criar um plano de backup programaticamente.

Também é possível executar as seguintes operações usando a API:

- Iniciar um trabalho de backup
- Descrever um trabalho de backup
- Obter metadados do ponto de recuperação
- Listar pontos de recuperação por recursos
- Listar tags para o ponto de recuperação

Visualizar backups de clusters do Amazon Redshift

Como visualizar e modificar seus backups de tabela do Amazon Redshift no console:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Escolha Cofres de backup. Depois, clique no nome do cofre de backup que contém seus clusters do Amazon Redshift.
3. O cofre de backup exibirá um resumo e uma lista de backups. É possível clicar no link na coluna ID do ponto de recuperação.
4. Para excluir um ou mais pontos de recuperação, marque a(s) caixa(s) que você deseja excluir. No botão Ações, selecione Excluir.

Restaurar um cluster do Amazon Redshift

Consulte como Restaurar um cluster do Amazon Redshift para obter mais informações.

Backups do Amazon Relational Database Service

Amazon RDS e AWS Backup

Ao considerar as opções para fazer backup de suas instâncias e clusters do Amazon RDS, é importante esclarecer qual tipo de backup você deseja criar e usar. Vários AWS recursos, incluindo o Amazon RDS, oferecem suas próprias soluções de backup nativas.

O Amazon RDS oferece a opção de fazer backups automáticos e manuais. Na terminologia do Amazon RDS, todos os pontos de recuperação criados pelo AWS Backup, inclusive aqueles em um plano de backup, estão considerando backups manuais.

Quando você usa AWS Backup para criar um backup (ponto de recuperação) de uma instância do Amazon RDS, AWS Backup verifica se você já usou o Amazon RDS para criar um backup automático. Se existir um backup automatizado, AWS Backup cria uma cópia desse instantâneo (`copy-db-snapshot`operação). Se nenhum backup existente existir, AWS Backup cria um instantâneo da instância indicada, em vez de uma cópia (`create-db-snapshot`operação).

O primeiro instantâneo feito por AWS Backup, criado por qualquer operação, resultará em 1 instantâneo completo. Todas as cópias subsequentes serão backups incrementais, desde que o backup completo exista.

> **Important**
>
> Quando um plano de AWS Backup backup é programado para criar vários instantâneos diários de uma instância do Amazon RDS e quando uma dessas janelas programadas de Início de AWS Backup Backup coincide com a janela de Backup do Amazon RDS, a linhagem de dados dos backups pode se ramificar em backups não idênticos, criando backups não planejados e conflitantes. Para evitar isso, certifique-se de que seu plano de AWS Backup backup ou a janela do Amazon RDS não coincidam em seus horários.

Backups contínuos e restauração pontual do Amazon RDS

Os backups contínuos envolvem o uso AWS Backup para criar um backup completo do seu recurso Amazon RDS e, em seguida, capturar todas as alterações por meio de um registro de transações.

Você pode obter uma granularidade maior retrocedendo até o momento em que deseja restaurar, em vez de escolher um instantâneo anterior tirado em intervalos de tempo fixos.

Consulte backups contínuos e serviços compatíveis com PITR e gerenciamento de configurações de backup contínuo para obter mais informações.

Backups Multi-AZ do Amazon RDS

AWS Backup faz backup e oferece suporte às opções de implantação do Amazon RDS for MySQL e PostgreSQL Multi-AZ (zona de disponibilidade) com uma instância de banco de dados primária e duas instâncias de banco de dados em espera legíveis.

Os backups Multi-AZ estão disponíveis nas seguintes regiões: Ásia-Pacífico (Sydney), Ásia-Pacífico (Tóquio), Europa (Irlanda), Leste dos EUA (Ohio), Oeste dos EUA (Oregon), Europa (Estocolmo), Ásia-Pacífico (Singapura), Leste dos EUA (Norte da Virgínia) e Europa (Frankfurt).

A opção de implantação Multi-AZ otimiza as transações de gravação e é ideal quando suas workloads exigem capacidade de leitura adicional, menor latência da transação de gravação, maior resiliência à instabilidade da rede (que afeta a consistência da latência da transação de gravação) e alta disponibilidade e durabilidade.

Para criar um cluster Multi-AZ, é possível escolher MySQL ou PostgreSQL como o tipo de mecanismo.

No AWS Backup console, há três opções de implantação:

- Cluster de banco de dados Multi-AZ: cria um cluster de banco de dados com uma instância de banco de dados primária e duas instâncias de banco de dados em espera legíveis. Cada instância de banco de dados em uma zona de disponibilidade diferente. Fornece alta disponibilidade, redundância de dados e aumenta a capacidade de workloads prontas para o servidor.
- Instância de banco de dados Multi-AZ: cria uma instância primária de banco de dados e uma instância de banco de dados em espera em uma zona de disponibilidade diferente. Isso fornece alta disponibilidade e redundância de dados, mas a instância de banco de dados em espera não é compatível com conexões para workloads de leitura.
- Instância de banco de dados única: cria uma única instância de banco de dados sem instâncias de banco de dados em espera.

Para criar um backup para o Amazon RDS, consulte Criar um backup para programar um backup como parte de seus planos de backup ou criar um backup sob demanda.

> **Note**
>
> A Recuperação para um ponto no tempo (PITR) pode ser compatível com as instâncias, mas não com os clusters.
> A cópia de um snapshot de cluster de banco de dados multi-AZ não é compatível.

Diferenças entre um cluster Multi-AZ e uma instância do RDS

Um backup em uma única zona de disponibilidade ou em duas zonas de disponibilidade é uma instância do RDS. Uma implantação e um backup com três ou mais instâncias são um cluster, semelhante aos clusters do Amazon Aurora, do Amazon Neptune e do Amazon DocumentDB.

O ARN (Nome do recurso da Amazon) é renderizado de forma diferente dependendo se a instância ou o cluster são usados:

Um ARN de instância do RDS: `arn:aws:rds:region: account:db:name`

Um cluster Multi-AZ do RDS: `arn:aws:rds:region:account :cluster:name`

Para obter mais informações, consulte Implantações de cluster de banco de dados Multi-AZ no Guia do usuário do Amazon RDS.

Para obter mais informações, sobre Criar um snapshot de cluster de banco de dados Multi-AZ, consulte o Guia do usuário do Amazon RDS.

AWS CloudFormation backups em pilha

Uma CloudFormation pilha consiste em vários recursos com e sem estado que você pode fazer backup como uma única unidade. Em outras palavras, é possível fazer backup e restaurar uma aplicação contendo vários recursos fazendo backup de uma pilha e restaurando os recursos dentro dela. Todos os recursos em uma pilha são definidos pelo modelo AWS CloudFormation dela.

Quando uma CloudFormation pilha é copiada, pontos de recuperação são criados para o CloudFormation modelo e para cada recurso adicional suportado AWS Backup na pilha. Esses pontos de recuperação são agrupados em um ponto de recuperação abrangente chamado composto.

Esse ponto de recuperação composto não pode ser restaurado, mas os pontos de recuperação aninhados podem ser restaurados. É possível restaurar de um a todos os backups aninhados em um backup composto usando o console ou a AWS CLI.

CloudFormation terminologia da pilha de aplicativos

- Ponto de recuperação composto: um ponto de recuperação usado para agrupar pontos de recuperação aninhados, bem como outros metadados.
- Ponto de recuperação aninhado: um ponto de recuperação de um recurso que faz parte de uma CloudFormation pilha e é copiado como parte do ponto de recuperação composto. Cada ponto de recuperação aninhado pertence à pilha de um ponto de recuperação composto.
- Trabalho composto: um trabalho de backup, cópia ou restauração de uma CloudFormation pilha que pode acionar outros trabalhos de backup para recursos individuais dentro da pilha.
- Trabalho aninhado: um trabalho de backup, cópia ou restauração de um recurso em uma AWS CloudFormation pilha.

CloudFormation tarefas de backup de pilha

O processo de criação de um backup é chamado de trabalho de backup. Uma tarefa de backup de CloudFormation pilha tem um status. Quando um trabalho de backup é concluído, ele tem o status de `Completed`. Isso significa que um AWS CloudFormation ponto de recuperação (um backup) foi criado.

CloudFormation as pilhas podem ser copiadas usando o console ou copiadas programaticamente. Para fazer backup de qualquer recurso, incluindo uma CloudFormation pilha, consulte Como criar um backup em outro lugar neste Guia AWS Backup do desenvolvedor.

CloudFormation as pilhas podem ser copiadas usando o comando `StartBackupJob` da API. Observe que a documentação e o console se referem a pontos de recuperação compostos e aninhados. A linguagem da API usa a terminologia “pontos de recuperação pai e filho” na mesma relação contextual.

CloudFormation as pilhas contêm todos os AWS recursos indicados pelo seu CloudFormation modelo. Observe que o modelo pode conter recursos que ainda não compatíveis com o AWS Backup. Se seu modelo contiver uma combinação de recursos AWS suportados e recursos não suportados, ainda AWS Backup fará backup do modelo em uma pilha composta, mas o Backup criará apenas pontos de recuperação dos serviços suportados pelo Backup. Todos os tipos de recursos contidos no CloudFormation modelo serão incluídos em um backup, mesmo que você não tenha optado por um serviço específico (alternando um serviço para “Ativado” nas configurações do console). É possível restaurar os backups aninhados (pontos de recuperação) compatíveis com o AWS Backup , mas não é possível fazer backup nem restaurar as pilhas aninhadas.

AWS CloudFormation ponto de recuperação

Status do ponto de recuperação

Quando o trabalho de backup de uma pilha é concluído (o status do trabalho é `Completed`), um backup da pilha é criado. Esse backup também é conhecido como ponto de recuperação composto. Um ponto de recuperação composto pode ter um dos seguintes status: `Completed`, `Failed` ou `Partial`. Observe que um trabalho de backup tem um status e um ponto de recuperação (também chamado de backup) também tem um status separado.

Uma tarefa de backup concluída significa que toda a sua pilha e os recursos nela contidos estão protegidos pelo AWS Backup. Um status de falha indica que o trabalho de backup não teve êxito. Você deverá criar o backup novamente quando o problema que causou a falha for corrigido.

Um status `Partial` significa que nem todos os recursos na pilha tiveram o backup feito. Isso pode acontecer se o CloudFormation modelo contiver recursos que não são atualmente suportados pelo AWS Backup, ou pode acontecer se uma ou mais das tarefas de backup pertencentes aos recursos dentro da pilha (recursos aninhados) tiverem status diferentes de. `Completed` É possível criar manualmente um backup sob demanda para executar novamente quaisquer recursos que resultaram em um status diferente de `Completed`. Se você esperava que a pilha tivesse o status de `Completed`, mas ela estiver marcada como `Partial`, verifique quais das condições acima podem ser verdadeiras em relação à pilha.

Cada recurso aninhado no ponto de recuperação composto tem seu próprio ponto de recuperação individual, cada um com seu próprio status (`Completed` ou `Failed`). É possível restaurar pontos de recuperação aninhados com status de `Completed`.

Gerenciar pontos de recuperação

É possível fazer backup dos pontos de recuperação compostos (backups). É possível fazer backup, excluir, desassociar ou restaurar os pontos de recuperação aninhados. Não é possível excluir um ponto de recuperação composto que contenha backups aninhados. Depois que os pontos de recuperação aninhados em um ponto de recuperação composto forem excluídos ou desassociados, você poderá excluir manualmente o ponto de recuperação composto ou deixá-lo permanecer até que o ciclo de vida do plano de backup o exclua.

Excluir um ponto de recuperação

Você pode excluir um ponto de recuperação usando o AWS Backup console ou usando AWS CLI o.

Para excluir pontos de recuperação usando o AWS Backup console,

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. clique em Recursos protegidos na navegação à esquerda. Na caixa de texto, digite `CloudFormation` para exibir somente suas CloudFormation pilhas.
3. Os pontos de recuperação compostos serão exibidos no painel Pontos de recuperação. É possível clicar no sinal de adição (+) à esquerda de cada ID de ponto de recuperação composto para expandi-lo, mostrando todos os pontos de recuperação aninhados contidos no composto. Marque a caixa à esquerda de qualquer ponto de recuperação para incluí-lo na seleção de pontos de recuperação que você deseja excluir.
4. Clique no botão Excluir.

Quando você usa o console para excluir um ou mais pontos de recuperação compostos, uma caixa de aviso será exibida. Essa caixa de aviso exige que você confirme sua intenção de excluir os pontos de recuperação compostos, incluindo os pontos de recuperação aninhados em pilhas compostas.

Para excluir pontos de recuperação usando a API, use o comando `DeleteRecoveryPoint`.

Ao usar a API com o, AWS Command Line Interface você deve excluir todos os pontos de recuperação aninhados antes de excluir um ponto composto. Se você enviar uma solicitação de API para excluir um backup de pilha composta (ponto de recuperação) que ainda contenha pontos de recuperação aninhados, a solicitação retornará um erro.

Desassociar um ponto de recuperação aninhado do ponto de recuperação composto

É possível dissociar um ponto de recuperação aninhado de um ponto de recuperação composto (por exemplo, você deseja manter o ponto de recuperação aninhado, mas excluir o ponto de recuperação composto). Os dois pontos de recuperação permanecerão, mas não estarão mais conectados. Ou seja, as ações que ocorrerem no ponto de recuperação composto não se aplicarão mais ao ponto de recuperação aninhado depois que ele for desassociado.

É possível desassociar o ponto de recuperação usando o console ou chamar a API `DisassociateRecoveryPointFromParent`. [Observe que as chamadas de API usam o termo “pai” para se referir aos pontos de recuperação compostos.]

Copiar um ponto de recuperação

Você pode copiar um ponto de recuperação composto ou copiar um ponto de recuperação aninhado se o recurso oferecer suporte à cópia entre contas e regiões.

Para copiar pontos de recuperação usando o AWS Backup console:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. clique em Recursos protegidos na navegação à esquerda. Na caixa de texto, digite `CloudFormation` para exibir somente suas CloudFormation pilhas.
3. Os pontos de recuperação compostos serão exibidos no painel Pontos de recuperação. É possível clicar no sinal de adição (+) à esquerda de cada ID de ponto de recuperação composto para expandi-lo, mostrando todos os pontos de recuperação aninhados contidos no composto. Clique no botão de círculo radial à esquerda de qualquer ponto de recuperação para copiá-lo.
4. Depois de selecionado, clique no botão Copiar no canto superior direito do painel.

Quando você copia um ponto de recuperação composto, os pontos de recuperação aninhados que não são compatíveis com a funcionalidade de cópia não irão para a pilha copiada. O ponto de recuperação composto terá um status de `Partial`.

Perguntas frequentes

1. “O que está incluído como parte do backup da aplicação?”

   Como parte de cada backup de um aplicativo definido usando CloudFormation, o modelo, o valor processado de cada parâmetro no modelo e os recursos aninhados suportados pelo AWS Backup são copiados. O backup de um recurso aninhado é feito da mesma forma que o backup de um recurso individual que não faz parte de uma CloudFormation pilha. Observe que os valores dos parâmetros marcados como `no-echo` não serão copiados.

2. “Posso fazer backup da minha AWS CloudFormation pilha que tem pilhas aninhadas?”

   Sim. Suas CloudFormation pilhas que contêm pilhas aninhadas podem estar em seu backup.

3. “Um status *`Partial`* significa que houve falha na criação do meu backup?”

   Não. Um status parcial indica que o backup de alguns dos pontos de recuperação foi feito, e não de outros. Há três condições para verificar se você esperava um resultado de backup `Completed`:

   a. Sua CloudFormation pilha contém recursos atualmente não suportados pelo? AWS Backup Para obter uma lista dos recursos compatíveis, consulte AWS Recursos compatíveis e aplicativos de terceiros em nosso Guia do desenvolvedor.

   b. Um ou mais trabalhos de backup pertencentes aos recursos da pilha não tiveram êxito e o trabalhos deve ser executado novamente.

c. Um ponto de recuperação aninhado foi excluído ou desassociado de um ponto de recuperação composto.

4. “Como excluo recursos do meu backup de CloudFormation pilha?”

   Ao fazer backup de sua CloudFormation pilha, você pode excluir recursos de fazerem parte do backup. No console, durante os processos de criar um plano de backup e atualizar um plano de backup, há uma etapa para atribuir recursos. Nessa etapa, há uma seção Seleção de recursos. Se você escolher incluir tipos de recursos específicos e incluí-los CloudFormation como recurso para backup, poderá excluir IDs de recursos específicos dos tipos de recursos selecionados. Também é possível usar tags para excluir recursos da pilha.

   Usando a CLI, você pode usar o

   - `NotResources`em seu plano de backup para excluir um recurso específico de suas CloudFormation pilhas.
   - `StringNotLike` para excluir itens por meio de tags.

5. “Quais tipos de backups são compatíveis com recursos aninhados?”

   Os backups de recursos aninhados podem ser completos ou incrementais, dependendo do tipo de backup suportado AWS Backup por esses recursos. Para obter mais informações, consulte Como funcionam os backups incrementais. No entanto, observe que a PITR (point-in-time restauração) não é compatível com os recursos aninhados do Amazon S3 e do Amazon RDS.

6. “Os conjuntos de alterações que fazem parte da CloudFormation pilha são copiados?”

   Não. O backup dos conjuntos de alterações não é feito como parte do backup da CloudFormation pilha.

7. “Como o status da AWS CloudFormation pilha afeta o backup?”

   O status da CloudFormation pilha pode afetar o backup. É possível fazer backup de uma pilha com um status que inclua `COMPLETE`, como os status `CREATE_COMPLETE`, `ROLLBACK_COMPLETE`, `UPDATE_COMPLETE`, `UPDATE_ROLLBACK_COMPLETE`, `IMPORT_COMPLETE` ou `IMPORT_ROLLBACK_COMPLETE`.

Caso haja falha no upload de um novo modelo e a pilha passe para o status de `ROLLBACK_COMPLETE`, o backup do novo modelo será feito, mas os backups dos recursos aninhados serão baseados nos recursos revertidos.

8. “Como os ciclos de vida da pilha de aplicações diferem dos ciclos de vida de outros pontos de recuperação?”

   Os ciclos de vida dos pontos de recuperação aninhados são determinados pelo plano de backup ao qual eles pertencem. O ponto de recuperação composto é determinado pelo ciclo de vida mais longo de todos os pontos de recuperação aninhados. Quando o último ponto de recuperação aninhado restante em um ponto de recuperação composto for excluído ou desassociado, o ponto de recuperação composto também será excluído.

9. “Como as etiquetas de um são CloudFormation copiadas para os pontos de recuperação?”

   Sim. Essas tags serão copiadas em cada respectivo ponto de recuperação aninhado.

10. “Existe uma ordem para excluir os pontos de recuperação compostos e aninhados (backups)?”

    Sim. Alguns backups devem ser excluídos antes que outros possam ser excluídos. Os backups compostos que contêm pontos de recuperação aninhados não podem ser excluídos até que todos os pontos de recuperação dentro do backup composto tenham sido excluídos. Quando um ponto de recuperação composto não tiver mais pontos de recuperação aninhados, você poderá excluí-lo manualmente. Caso contrário, ele será excluído de acordo com o ciclo de vida do plano de backup.

Restaurar aplicativos em uma pilha

Consulte Como restaurar backups da pilha de aplicações para obter informações sobre como restaurar pontos de recuperação aninhados.

Criar backups do VSS do Windows

Com isso AWS Backup, você pode fazer backup e restaurar aplicativos Windows habilitados para VSS (Volume Shadow Copy Service) executados em instâncias do Amazon EC2. Se o aplicativo tiver um gravador VSS registrado no Windows VSS, AWS Backup criará um instantâneo que será consistente para esse aplicativo.

Você pode realizar restaurações consistentes enquanto usa o mesmo serviço de backup gerenciado usado para proteger outros AWS recursos. Com backups do Windows consistentes com aplicações no EC2, você obtém as mesmas configurações de consistência e reconhecimento de aplicações que as ferramentas de backup tradicionais.

> **Note**
>
> AWS Backup atualmente, só oferece suporte a backups consistentes com aplicativos de recursos executados no Amazon EC2, especificamente cenários de backup em que os dados do aplicativo podem ser restaurados substituindo uma instância existente por uma nova instância criada a partir do backup. Não há compatibilidade com todos os tipos de instância ou de aplicações para backups do VSS do Windows.

Para obter mais informações, consulte Criação de um snapshot consistente com o aplicativo VSS no Guia do usuário do Amazon EC2.

Para fazer backup e restaurar recursos do Windows habilitados para VSS executados no Amazon EC2, siga estas etapas para concluir as tarefas de pré-requisito necessárias. Para obter instruções, consulte Antes de começar no Guia do usuário do Amazon EC2 para instâncias do Windows.

1. Baixe, instale e configure o agente SSM em AWS Systems Manager. Essa etapa é necessária. Para obter instruções, consulte Como trabalhar com o agente SSM em instâncias do Amazon EC2 para Windows Server no Guia do usuário do Systems AWS Manager.
2. Adicione uma política do IAM ao perfil do IAM e anexe o perfil à instância do Amazon EC2 antes de fazer o backup do VSS (Serviço de Cópias de Sombra de Volume) do Windows. Para obter instruções, consulte Criar uma função do IAM para snapshots habilitados para VSS no Guia do usuário do Amazon EC2. Para ver um exemplo de política do IAM, consulte Políticas gerenciadas para AWS Backup.
3. Fazer download e instale os componentes do VSS na instância do Windows no EC2
4. Habilite o VSS em: AWS Backup
    1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
    2. No painel, escolha o tipo de backup que você deseja criar: Criar um backup sob demanda ou Gerenciar planos de backup. Forneça as informações necessárias para o tipo de backup.
    3. Ao atribuir recursos, escolha EC2. No momento, o backup do VSS é compatível somente com instâncias do EC2.

4. Na seção Configurações avançadas, escolha VSS do Windows. Isso permite que você faça backups do VSS do Windows.
5. Crie o backup.

Um trabalho de backup com o status de `Completed` não garante que a parte do VSS tenha êxito. A inclusão do VSS é feita com base no melhor esforço. Prossiga com as etapas a seguir para determinar se um backup é consistente com a aplicação, consistente em caso de falha ou com falha:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Em Minha conta, no painel de navegação esquerdo, clique em Trabalhos.
3. O status de `Completed` indica um trabalho com êxito que é consistente com a aplicação (VSS).

   Um status de `Completed with issues` indica que houve falha na operação do VSS, portanto, somente um backup consistente em caso de falha teve êxito. Esse status também terá uma mensagem pop-over "`Windows VSS Backup Job Error encountered, trying for regular backup`".

   Se o backup não tiver êxito, o status será `Failed`.
4. Para visualizar detalhes adicionais do trabalho de backup, clique no trabalho individual. Por exemplo, os detalhes podem ser `Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation`.

Backups habilitados para VSS com um destino que não seja Windows ou componente não VSS. O trabalho bem-sucedido do Windows será consistente com falhas sem o VSS.

Instâncias do Amazon EC2 incompatíveis

Os seguintes tipos de instância do Amazon EC2 não são compatíveis com backups do Windows habilitados para VSS porque são instâncias pequenas e podem não fazer o backup com êxito.

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

Amazon EBS e AWS Backup

O processo de backup dos recursos do Amazon EBS é semelhante às etapas usadas para fazer backup de outros tipos de recursos:

- Criar um backup sob demanda
- Criar um backup programado

As informações específicas para cada recurso são indicadas nas seções a seguir.

Nível de arquivamento do Amazon EBS para armazenamento frio

O EBS é um dos recursos que oferecem suporte à transição de backups para armazenamento frio. Para ter mais informações, consulte Ciclo de vida e níveis de armazenamento.

> **Note**
>
> Esse recurso não está disponível nas regiões China (Pequim), China (Ningxia), AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA).

Backups multivolume e consistentes em caso de falha do Amazon EBS

Por padrão, AWS Backup cria backups consistentes em caso de falhas dos volumes do Amazon EBS que estão conectados a uma instância do Amazon EC2. A consistência em caso de falha significa que os snapshots de cada volume do Amazon EBS anexado à mesma instância do Amazon EC2 são tirados exatamente no mesmo momento. Você não precisa mais interromper suas instâncias ou coordenar entre vários volumes do Amazon EBS para garantir a consistência em caso de falha do estado da sua aplicação.

Como instantâneos de vários volumes e consistentes com falhas são uma AWS Backup funcionalidade padrão, você não precisa fazer nada diferente para usar esse recurso. Você pode fazer backup de volumes do Amazon EBS usando um dos seguintes procedimentos:

A função usada para criar um ponto de recuperação de snapshot do EBS será associada a esse snapshot. Essa mesma função deve ser usada para excluir pontos de recuperação criados por ela ou para fazer a transição de pontos de recuperação para uma camada de arquivamento.

Bloqueio de snapshot do Amazon EBS e AWS Backup

AWS Backup snapshots gerenciados do Amazon EBS e snapshots associados a uma AMI gerenciada do AWS Backup Amazon EC2 que tenham o Amazon EBS Snapshot Lock aplicado não podem ser excluídos como parte do ciclo de vida do ponto de recuperação se a duração do bloqueio do snapshot exceder o ciclo de vida do backup. Em vez disso, esses pontos de recuperação terão um status de `EXPIRED`. Esses pontos de recuperação poderão ser excluídos manualmente se você optar por começar removendo o Bloqueio de Snapshots do Amazon EBS.

Restaurar recursos do Amazon EBS

Para restaurar seus volumes do Amazon EBS, siga as etapas em Restaurar um volume do Amazon EBS.

Copiar tags em backups

Em geral, AWS Backup copia as tags dos recursos que ela protege para seus pontos de recuperação. Para obter mais informações sobre como copiar tags durante uma restauração, consulte Copiar tags durante uma restauração.

Por exemplo, quando você faz backup de um volume do Amazon EC2, AWS Backup copia suas tags de grupo e de recursos individuais para o snapshot resultante, de acordo com o seguinte:

- Para obter uma lista de permissões específicas do recurso que são necessárias para salvar tags de metadados em backups, consulte Permissões necessárias para atribuir tags a backups.
- As tags originalmente associadas a um recurso e as tags atribuídas durante o backup são atribuídas aos pontos de recuperação armazenados em um cofre de backup, até um máximo de 50 (essa é uma AWS limitação). As tags atribuídas durante o backup têm prioridade, e os dois conjuntos de tags são copiados em ordem alfabética.
- O DynamoDB não é compatível com a atribuição de tags aos backups, a menos que você habilite Backup avançado do DynamoDB primeiro.
- Os volumes do Amazon EBS anexados às instâncias do Amazon EC2 são recursos aninhados. As tags nos volumes do Amazon EBS que estão anexados às instâncias do Amazon EC2 são tags aninhadas. AWS Backup faz o possível para copiar as tags aninhadas, mas se não for bem-sucedida, ela cria um backup sem elas e relata o Status Concluído.
- Quando um backup do Amazon EC2 cria um ponto de recuperação de imagem e um conjunto de snapshots, AWS Backup copia as tags para a AMI resultante. AWS Backup também se esforça

ao máximo para copiar as tags dos volumes associados à instância do Amazon EC2 para os snapshots resultantes.

Se você copiar seu backup para outro Região da AWS, AWS Backup copiará todas as tags do backup original para o destino Região da AWS.

Interromper um trabalho de backup

Você pode interromper uma tarefa de backup AWS Backup depois que ela for iniciada. Quando você fizer isso, o backup não será criado e o registro do trabalho de backup será retido com o status abortado.

Para interromper um trabalho de backup usando o AWS Backup console

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Trabalhos.
3. Escolha o trabalho de backup que você deseja interromper.
4. No painel de detalhes do trabalho de backup, escolha Interromper.

Copiar um backup

Você pode copiar backups para vários, sob demanda Contas da AWS ou Regiões da AWS automaticamente como parte de um plano de backup programado para a maioria dos tipos de recursos. Para obter detalhes, consultethe section called “Disponibilidade de recursos por recurso”.

Também é possível automatizar uma sequência de cópias entre contas e entre regiões para a maioria dos recursos compatíveis, exceto para o Amazon RDS e o Aurora. Para snapshots do Amazon RDS e do Aurora AWS Backup , só é possível automatizar cópias entre contas ou entre regiões devido à forma como esses serviços criam suas chaves de criptografia (não há suporte para copiar um snapshot de cluster de banco de dados Multi-AZ).

Alguns tipos de recursos têm a capacidade de backup contínuo e de cópia entre contas e entre regiões disponível. Quando uma cópia entre regiões ou entre contas de um backup contínuo é feita, o ponto de recuperação copiado (backup) se torna um backup de snapshot (periódico). Dependendo do tipo de recurso, os instantâneos podem ser uma cópia incremental ou uma cópia completa. A PITR (para um ponto no tempo) não está disponível para essas cópias.

As cópias mantêm sua configuração de origem, incluindo datas de criação e período de retenção. A data de criação se refere a quando a fonte foi criada, não quando a cópia foi criada.

OBSERVAÇÃO: a configuração de origem substitui a configuração de expiração da cópia, mesmo que a cópia esteja definida para nunca expirar. Uma cópia definida para nunca expirar ainda manterá a data de expiração da origem.

Se você quiser que a nova cópia de backup nunca expire, defina seus backups de origem para nunca expirar ou então determine que a nova cópia expirará 100 anos após a criação.

Conteúdo

Criação de cópias de backup em Regiões da AWS

Usando AWS Backup, você pode copiar backups para vários, Regiões da AWS sob demanda ou automaticamente, como parte de um plano de backup agendado. A replicação entre regiões é particularmente valiosa se você tiver requisitos de continuidade dos negócios ou de conformidade para armazenar backups a uma distância mínima dos dados de produção. Para assistir a um tutorial em vídeo, consulte Gerenciar cópias de backup entre regiões.

Quando você copia um backup para um novo Região da AWS pela primeira vez, AWS Backup copia o backup na íntegra. Em geral, se um serviço oferecer suporte a backups incrementais, as cópias subsequentes desse backup no mesmo Região da AWS serão incrementais. AWS Backup criptografará novamente sua cópia usando a chave gerenciada pelo cliente do seu cofre de destino.

Uma exceção é o Amazon EBS, que afirma que a alteração do status de criptografia de um snapshot durante uma operação de cópia resulta em uma cópia completa (não incremental).

Requisitos

- A maioria dos recursos AWS Backup suportados oferece suporte ao backup entre regiões. Para obter detalhes, consulte Disponibilidade de recursos por recurso.
- A maioria das AWS regiões oferece suporte ao backup entre regiões. Para obter detalhes, consulte Disponibilidade de recursos por Região da AWS.
- AWS Backup não oferece suporte a cópias entre regiões para armazenamento em camadas frias.

Considerações sobre cópia entre regiões com recursos específicos

Amazon RDS

Você não pode copiar um grupo de opções para outro Região da AWS. Se isso acontecer, você poderá receber um erro, como “O snapshot requer um grupo de opções de destino com as seguintes opções:...”

Você deve inserir os mesmos grupos de opções no destino Região da AWS ao criar uma nova cópia entre regiões de um snapshot do Amazon RDS.

Executar backup sob demanda entre regiões

Como copiar um backup sob demanda existente

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Escolha Cofres de backup.
3. Escolha o cofre que contenha o ponto de recuperação que você deseja copiar.
4. Na seção Backups, selecione o ponto de recuperação a ser copiado.
5. Usando o botão suspenso Ações, escolha Copiar.
6. Insira os seguintes valores:

   Copiar no destino

   Escolha o Região da AWS destino da cópia. Você pode adicionar uma nova regra de cópia por cópia em um novo destino.

   Cofre de backup de destino

   Escolha o cofre de backup de destino para a cópia.

   Transição para o armazenamento frio

   Escolha quando fazer a transição da cópia de backup para o armazenamento frio. Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Esse valor não pode ser alterado após a transição de uma cópia para o armazenamento estático.

   Para ver a lista de recursos que podem fazer a transição para o armazenamento frio, consulte a seção “Ciclo de vida até o armazenamento frio” da tabela Disponibilidade de recursos por recurso. A expressão de armazenamento frio é ignorada para outros recursos.

Período de retenção

Escolha Especifica o número de dias em que a cópia é excluída depois de sua criação. Esse valor deve ser superior a 90 dias além do valor de Transição para armazenamento estático. O período de retenção Sempre retém a cópia indefinidamente.

IAM role (Perfil do IAM)

Escolha a função do IAM que AWS Backup será usada ao criar a cópia. A função também deve estar AWS Backup listada como uma entidade confiável, o que AWS Backup permite assumir a função. Se você escolher Padrão e a função AWS Backup padrão não estiver presente na sua conta, uma será criada para você com as permissões corretas.

7. Escolha Copiar.

Programar o backup entre regiões

É possível usar um plano de backup programado para copiar backups entre Regiões da AWS.

Como copiar um backup usando um plano de backup programado

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Em Minha conta, escolha Planos de backup e, depois, escolha Criar plano de backup.
3. Na página Criar plano de Backup, escolha Criar um plano.
4. Em Nome do plano de backup, insira um nome para o plano.
5. Na seção Configuração da regra de backup, adicione uma regra de backup que defina uma programação de backup, uma janela de backup e regras de ciclo de vida. Você poderá adicionar mais regras de backup posteriormente.
   a. Em Nome da regra de backup, insira um nome para a regra.
   b. Em Cofre de backup, escolha um cofre na lista. Os pontos de recuperação desse backup serão salvos nesse cofre. É possível criar um cofre de backup.
   c. Em Frequência de backup, escolha com que frequência você deseja fazer backups.
   d. Para serviços que suportam PITR, se você quiser esse recurso, escolha Habilitar backups contínuos para point-in-time recuperação (PITR). Para obter uma lista de serviços compatíveis com a PITR, consulte essa seção da tabela Disponibilidade de recursos por recurso.

e. Em Janela de backup, escolha Usar padrões da janela de backup – recomendado. É possível personalizar a janela de backup.

f. Em Copiar no destino, escolha a Região da AWS de destino para a cópia de backup. O backup será copiado nessa região. Você pode adicionar uma nova regra de cópia por cópia em um novo destino. Insira os seguintes valores:

Copiar no cofre de outra conta

Não ative essa opção. Para saber mais sobre cópia entre contas, consulte Criação de cópias de backup em Contas da AWS

Cofre de backup de destino

Escolha o cofre de backup na região de destino onde AWS Backup copiará seu backup.

Se você quiser criar um cofre de backup para a cópia entre regiões, escolha Criar cofre de backup. Insira as informações no assistente. Depois, escolha Criar cofre de backup.

6. Selecione Criar plano.

Criação de cópias de backup em Contas da AWS

Usando AWS Backup, você pode fazer backup de vários sob Contas da AWS demanda ou automaticamente como parte de um plano de backup programado. Use um backup entre contas se quiser copiar com segurança seus backups para uma ou mais pessoas Contas da AWS em sua organização por motivos operacionais ou de segurança. Se o backup original for excluído acidentalmente, você poderá copiar o backup da conta de destino para a conta de origem e, em seguida, iniciar a restauração. Antes de fazer isso, é preciso ter duas contas que pertençam à mesma organização no serviço AWS Organizations . Para obter mais informações, consulte Criar e configurar uma organização no Guia do usuário do Organizations.

Na sua conta de destino, crie um cofre de backup. Em seguida, você atribui uma chave gerenciada pelo cliente para criptografar os backups na conta de destino e uma política de acesso baseada em recursos para permitir o acesso AWS Backup aos recursos que você gostaria de copiar. Na conta de origem, se os recursos estiverem criptografados com uma chave gerenciada pelo cliente, você deverá compartilhar essa chave com a conta de destino. Depois, você poderá criar um plano de backup e escolher uma conta de destino que faça parte da sua unidade organizacional no AWS Organizations.

Quando você copia um backup para várias contas pela primeira vez, AWS Backup copia o backup na íntegra. Em geral, se um serviço oferecer suporte a backups incrementais, as cópias subsequentes desse backup na mesma conta serão incrementais. AWS Backup criptografa novamente sua cópia usando a chave gerenciada pelo cliente do seu cofre de destino.

Requisitos

- Antes de gerenciar recursos Contas da AWS em vários estados AWS Backup, suas contas devem pertencer à mesma organização no AWS Organizations serviço.
- A maioria dos recursos suportados pelo AWS Backup suporte oferece suporte ao backup entre contas. Para obter detalhes, consulte Disponibilidade de recursos por recurso.
- A maioria das AWS regiões oferece suporte ao backup entre contas. Para obter detalhes, consulte Disponibilidade de recursos por Região da AWS.
- AWS Backup não oferece suporte a cópias entre contas para armazenamento em camadas frias.

Configurar o backup entre contas

O que é necessário para criar backups entre contas?

- Uma conta de origem

  A conta de origem é a conta em que residem seus AWS recursos de produção e backups principais.

  O usuário da conta de origem inicia a operação de backup entre contas. O usuário ou o perfil da conta de origem devem ter as permissões de API apropriadas para iniciar a operação. As permissões apropriadas podem ser a política AWS gerenciada`AWSBackupFullAccess`, que permite acesso total às AWS Backup operações, ou uma política gerenciada pelo cliente que permite ações como`ec2:ModifySnapshotAttribute`. Para obter mais informações sobre os tipos de política, consulte Políticas gerenciadas pelo AWS Backup.
- Uma conta de destino

  A conta de destino é a conta na qual você deseja manter uma cópia do seu backup. É possível escolher mais de uma conta de destino. A conta de destino deve estar na mesma organização que a conta de origem no AWS Organizations.

Você deve “Permitir” a política de acesso ao `backup:CopyIntoBackupVault` para o seu cofre de backup de destino. A ausência dessa política negará as tentativas de copiar na conta de destino.

- Uma conta de gerenciamento em AWS Organizations

  A conta de gerenciamento é a conta principal na sua organização, conforme definido pelo AWS Organizations, que você usa para gerenciar o backup entre contas entre suas Contas da AWS. Para usar o backup entre contas, também é necessário habilitar a confiança do serviço. Depois de habilitar a confiança do serviço, você poderá usar qualquer conta na organização como uma conta de destino. Na sua conta de destino, escolha quais cofres usar para o backup entre contas.
- Habilitar o backup entre contas no console do AWS Backup

Para obter mais informações sobre a segurança, consulte Considerações de segurança para backup entre contas.

Para usar o backup entre contas, você deve habilitar o recurso de backup entre contas. Depois, você deverá “Permitir” a política de acesso ao `backup:CopyIntoBackupVault` no seu cofre de backup de destino.

Ativar backup entre contas

1. Faça login usando as credenciais AWS Organizations da sua conta de gerenciamento. O backup entre contas só poderá ser habilitado ou desabilitado usando essas credenciais.
2. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
3. Em Minha conta, escolha Configurações.
4. Em Backup entre contas, escolha Habilitar.
5. Em Cofres de backup, escolha o cofre de destino.

   Para cópia entre contas, o cofre de origem e o cofre de destino estão em contas diferentes. Mude para a conta que possui a conta de destino, conforme necessário.
6. Na seção Política de acesso, “Permita” o `backup:CopyIntoBackupVault`. Por exemplo, escolha Adicionar permissões e, depois, Permitir acesso a um cofre de Backup da organização. Qualquer ação entre contas que não seja `backup:CopyIntoBackupVault` será rejeitada.
7. Agora, qualquer conta na sua organização poderá compartilhar o conteúdo de seu cofre de backup com qualquer outra conta na organização. Para ter mais informações, consulte Compartilhar um cofre de backup com uma conta da AWS diferente. Para limitar quais contas

podem receber o conteúdo dos cofres de backup de outras contas, consulte Configurar sua conta como uma conta de destino.

Programar o backup entre contas

É possível usar um plano de backup programado para copiar backups entre Contas da AWS.

Como copiar um backup usando um plano de backup programado

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Em Minha conta, escolha Planos de backup e, depois, escolha Criar plano de backup.
3. Na página Criar plano de Backup, escolha Criar um plano.
4. Em Nome do plano de backup, insira um nome para o plano.
5. Na seção Configuração da regra de backup, adicione uma regra de backup que defina uma programação de backup, uma janela de backup e regras de ciclo de vida. Você poderá adicionar mais regras de backup posteriormente.

   Em Nome da regra, insira um nome para a regra.
6. Na seção Programar, em Frequência, escolha com que frequência você deseja que o backup seja feito.
7. Em Janela de backup, escolha Usar padrões da janela de backup (recomendado). É possível personalizar a janela de backup.
8. Em Cofre de backup, escolha um cofre na lista. Os pontos de recuperação desse backup serão salvos nesse cofre. É possível criar um cofre de backup.
9. Na seção Gerar cópia – opcional, insira os seguintes valores:

   Região de destino

   Escolha o destino Região da AWS para sua cópia de backup. O backup será copiado nessa região. Você pode adicionar uma nova regra de cópia por cópia em um novo destino.

   Copiar no cofre de outra conta

   Alterne para escolher essa opção. A opção ficará azul quando selecionada. A opção ARN do cofre externo será exibida.

ARN do cofre externo

O nome do recurso da Amazon (ARN) da conta de destino. O ARN é uma sequência de caracteres que contém o ID da conta e seus. Região da AWS AWS Backup copiará o backup para o cofre da conta de destino. A lista de regiões de destino é atualizada automaticamente com a região no ARN do cofre externo.

Em Permitir acesso ao cofre do Backup, escolha Permitir. Depois, escolha Permitir no assistente que será aberto.

AWS Backup precisa de permissões para acessar a conta externa para copiar o backup para o valor especificado. O assistente mostra o seguinte exemplo de política que fornece esse acesso.

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

Transição para o armazenamento frio

Escolha quando fazer a transição da cópia de backup para o armazenamento estático e quando expirar (excluir) a cópia. Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Esse valor não pode ser alterado após a transição de uma cópia para o armazenamento estático.

Para ver a lista de recursos que podem fazer a transição para o armazenamento frio, consulte a seção “Ciclo de vida até o armazenamento frio” da tabela Disponibilidade de recursos por recurso. A expressão de armazenamento frio é ignorada para outros recursos.

Expirar especifica o número de dias em que a cópia é excluída depois de sua criação. Esse valor deve ser superior a 90 dias além do valor de Transição para armazenamento estático.

> **Note**
>
> Quando os backups expiram e são marcados para exclusão como parte de sua política de ciclo de vida, AWS Backup exclui os backups em um ponto escolhido aleatoriamente nas 8 horas seguintes. Essa janela ajuda a garantir um desempenho consistente.

10. Escolha Tags adicionadas aos pontos de recuperação para adicionar tags aos seus pontos de recuperação.
11. Em configurações avançadas de backup, escolha VSS do Windows para habilitar snapshots com reconhecimento de aplicações para o software de terceiros selecionado em execução no EC2.
12. Selecione Criar plano.

Executar backup sob demanda entre contas

Você pode copiar um backup para Conta da AWS outro sob demanda.

Como copiar um backup sob demanda

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Em Minha conta, escolha Cofre de backup para ver todos os seus cofres de backup listados. É possível filtrar pelo nome ou tag do cofre de backup.
3. Escolha o ID do ponto de recuperação do backup que deseja copiar.
4. Escolha Copiar.
5. Expanda os Detalhes do backup para ver as informações sobre o ponto de recuperação que você está copiando.
6. Na seção Configuração de cópia, escolha uma opção na lista Região de destino.
7. Escolha Copiar no cofre de outra conta. A opção ficará azul quando selecionada.
8. O nome do recurso da Amazon (ARN) da conta de destino. O ARN é uma sequência de caracteres que contém o ID da conta e seus. Região da AWS AWS Backup copiará o backup

para o cofre da conta de destino. A lista de regiões de destino é atualizada automaticamente com a região no ARN do cofre externo.

9. Em Permitir acesso ao cofre do Backup, escolha Permitir. Depois, escolha Permitir no assistente que será aberto.

   Para criar a cópia, AWS Backup precisa de permissões para acessar a conta de origem. O assistente mostra o seguinte exemplo de política que fornece esse acesso. Esta política é mostrada a seguir.

```
{
  "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. Em Transição para armazenamento frio, escolha quando fazer a transição da cópia de backup para o armazenamento frio e quando expirar (excluir) a cópia. Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Esse valor não pode ser alterado após a transição de uma cópia para o armazenamento estático.

    Para ver a lista de recursos que podem fazer a transição para o armazenamento frio, consulte a seção “Ciclo de vida até o armazenamento frio” da tabela Disponibilidade de recursos por recurso. A expressão de armazenamento frio é ignorada para outros recursos.

    Expirar especifica o número de dias em que a cópia é excluída depois de sua criação. Esse valor deve ser superior a 90 dias além do valor de Transição para armazenamento estático.

11. Em perfil do IAM, especifique o perfil do IAM (como a função padrão) que tem as permissões para disponibilizar seu backup para cópia. O ato de copiar é realizado pela função vinculada ao serviço da sua conta de destino.

12. Escolha Copiar. Dependendo do tamanho do recurso que está copiando, esse processo pode levar várias horas para ser concluído. Quando o trabalho de cópia for concluído, você verá a cópia na guia Trabalhos de cópia no menu Trabalhos.

Chaves de criptografia e cópias entre contas

A chave de criptografia de cópia entre contas depende do tipo de recurso. Recursos que AWS Backup Gerenciamento completo usaram a chave de criptografia do cofre de backup de origem. As chaves KMS gerenciadas pelo cliente podem ser usadas para criptografia de cópias entre contas desses tipos de recursos.

Os tipos de recursos que não são totalmente gerenciados por AWS Backup têm a mesma chave KMS de origem e chave KMS de recurso. A cópia entre contas com chaves KMS AWS gerenciadas não é suportada para esses tipos de recursos que não são totalmente gerenciados pelo. AWS Backup

Para obter ajuda adicional na solução de falhas de cópia entre contas, consulte o Centro de AWS Conhecimento.

Durante uma cópia entre contas, a política de chaves KMS da conta de origem deve permitir a conta de destino na política de chaves KMS.

Restaurando um backup de um Conta da AWS para outro

AWS Backup não suporta a recuperação de recursos de um Conta da AWS para outro. No entanto, é possível copiar um backup de uma conta para outra conta e depois restaurá-lo nessa conta. Por exemplo, você não pode restaurar um backup da conta A para a conta B, mas pode copiar um backup da conta A para a conta B e depois restaurá-lo na conta B.

Restaurar um backup de uma conta para outra é um processo em duas etapas.

Como restaurar um backup de uma conta da para outra

1. Copie o backup da origem Conta da AWS para a conta para a qual você deseja restaurar. Para obter instruções, consulte Configurar o backup entre contas.
2. Use as instruções apropriadas para seu recurso para restaurar o backup.

Compartilhar um cofre de backup com uma conta da AWS diferente

AWS Backup permite que você compartilhe um cofre de backup com uma ou várias contas, ou com toda a sua organização em AWS Organizations. É possível compartilhar um cofre de backup de destino com uma conta da AWS de origem, um usuário ou um perfil do IAM.

Como compartilhar um cofre de backup de destino

1. Escolha AWS Backup e, depois, escolha Cofres de Backup.
2. Escolha o nome do cofre de backup que você deseja compartilhar.
3. No painel Política de acesso, escolha o menu suspenso Adicionar permissões.
4. Escolha Permitir acesso em nível de conta a um cofre de Backup. Ou você pode optar por permitir o acesso no nível da organização ou do perfil.
5. Insira o AccountID da conta que você deseja compartilhar com esse cofre de backup de destino.
6. Escolha Salvar política.

Você pode usar políticas do IAM para compartilhar o cofre de backup.

Compartilhar um cofre de backup de destino com uma Conta da AWS ou comum perfil do IAM

A política a seguir compartilha um cofre de backup com o número de conta `4444555566666` e o perfil do IAM `SomeRole` no número de conta `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":"*"
    }
  ]
}
```

Compartilhe um cofre de backup de destino em uma unidade organizacional AWS Organizations

A política a seguir compartilha um cofre de backup com unidades organizacionais que usam seus `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/*"
          ]
        }
      }
    }
  ]
}
```

Compartilhe um cofre de backup de destino com uma organização no AWS Organizations

A política a seguir compartilha um cofre de backup com a organização com `PrincipalOrgID` “o-a1b2c3d4e5".

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
```

```
        }
      }
    }
  ]
}
```

Configurar sua conta como uma conta de destino

Quando você ativa pela primeira vez os backups entre contas usando sua conta de AWS Organizations gerenciamento, qualquer usuário de uma conta membro pode configurar sua conta para ser uma conta de destino. Recomendamos a configuração de uma ou mais das seguintes políticas de controle de serviço (SCPs) no AWS Organizations para limitar as contas de destino. Para saber mais sobre como anexar políticas de controle de serviço aos AWS Organizations nós, consulte Anexando e desanexando políticas de controle de serviço.

Limitar contas de destino usando tags

Quando anexada a uma conta AWS Organizations raiz, OU ou individual, essa política limita os destinos de cópias dessa raiz, OU ou conta somente para as contas com cofres de backup que você marcou. `DestinationBackupVault` A permissão `"backup:CopyIntoBackupVault"` controla como um cofre de backup se comporta e, nesse caso, quais cofres de backup de destino são válidos. Use essa política, junto com a tag correspondente aplicada aos cofres de destino aprovados, para controlar os destinos das cópias entre contas somente para contas e cofres de backup aprovados.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
    }
  ]
}
```

Limitar as contas de destino usando números de conta e nomes de cofres

Quando anexada a uma conta AWS Organizations raiz, OU ou individual, essa política limita as cópias originadas dessa raiz, OU ou conta a apenas duas contas de destino. A permissão `"backup:CopyFromBackupVault"` controla o comportamento de um ponto de recuperação no cofre de backup e, nesse caso, os destinos nos quais você pode copiar esse ponto de recuperação. O cofre de origem só permitirá cópias na primeira conta de destino (112233445566) se um ou mais nomes de cofres de backup de destino começarem com `cab-`. O cofre de origem só permitirá cópias na segunda conta de destino (123456789012) se o destino for o cofre de backup chamado `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 as contas de destino usando unidades organizacionais no AWS Organizations

Quando anexada a uma AWS Organizations raiz ou OU que contém sua conta de origem, ou quando vinculada à sua conta de origem, a política a seguir limita as contas de destino às contas dentro das duas OUs 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/*"
          ]
        }
      }
    }
  ]
}
```

Considerações de segurança para backup entre contas

Esteja ciente do seguinte ao usar backups entre contas no AWS Backup:

- O cofre de destino não pode ser o cofre padrão. Isso ocorre porque o cofre padrão foi criptografado com uma chave que não pode ser compartilhada com outras contas.
- Os backups entre contas poderão ainda ser executados por até 15 minutos após a desativação do backup entre contas. Isso ocorre devido a uma eventual consistência e poderá resultar no início ou na conclusão de alguns trabalhos entre contas, mesmo após a desativação do backup entre contas.
- Se a conta de destino deixar a organização em uma data posterior, essa conta reterá os backups. Para evitar possíveis vazamentos de dados, coloque uma permissão de negação na permissão `organizations:LeaveOrganization` em uma política de controle de serviço (SCP) anexada à conta de destino. Para obter informações detalhadas sobre SCPs, consulte Remover uma conta-membro da sua organização no Guia do usuário do Organizations.
- Se você excluir uma função de trabalho de cópia durante uma cópia entre contas, não AWS Backup poderá cancelar o compartilhamento de instantâneos da conta de origem quando o trabalho de cópia for concluído. Nesse caso, o trabalho de backup será concluído, mas o status do trabalho de cópia será exibido como Falha ao cancelar o compartilhamento do snapshot.

Excluir backups

Recomendamos que você AWS Backup exclua automaticamente os backups de que não precisa mais, configurando seu ciclo de vida ao criar seu plano de backup. Por exemplo, se você definir o ciclo de vida do seu plano de backup para reter seus pontos de recuperação por um ano, AWS Backup excluirá automaticamente em 1º de janeiro de 2022 os pontos de recuperação criados em ou

dentro de algumas horas a partir de 1º de janeiro de 2021. (AWS Backup randomiza suas exclusões dentro de 8 horas após a expiração do ponto de recuperação para manter o desempenho.) Para saber mais sobre como configurar sua política de retenção do ciclo de vida, consulte Criar um plano de backup.

No entanto, talvez você queira excluir manualmente um ou mais pontos de recuperação. Por exemplo: .

- Você tem pontos de recuperação `EXPIRED`. Esses são pontos de recuperação AWS Backup que não puderam ser excluídos automaticamente porque você excluiu ou modificou a política original do IAM usada para criar seu plano de backup. Quando AWS Backup tentei excluí-los, faltou permissão para fazer isso.

  Pontos de recuperação expirados também podem ser criados se um ponto de recuperação AWS gerenciado do Amazon EBS ou do Amazon EC2 tiver um Amazon EBS Snapshot Lock aplicado AWS Backup e não conseguir concluir o processo do ciclo de vida que normalmente resultaria na exclusão do ponto de recuperação. Observe que esses pontos de recuperação expirados podem ser restaurados pelo console e pela API do Amazon EC2 ou pelo console e pela API do Amazon EBS.

  > **Warning**
  >
  > Você continuará armazenando pontos de recuperação expirados em sua conta. Isso pode aumentar seus custos de armazenamento.

  Depois de 6 de agosto de 2021, AWS Backup mostrará o ponto de recuperação de destino como expirado em seu cofre de backup. Você pode passar o mouse sobre o status Expirado em vermelho para ver uma mensagem de status pop-over que explica por que não foi possível excluir o backup. Também é possível escolher Atualizar para receber as informações mais recentes.
- Você não quer mais que um plano de backup opere da maneira como foi configurado. Atualizar o plano de backup afeta os futuros pontos de recuperação que ele criará, mas não afeta o ponto de recuperação que ele já tiver criado. Para saber mais, consulte Atualizar um plano de backup.
- É necessário fazer uma limpeza depois que você terminar um teste ou tutorial.

Excluir backups manualmente

Como excluir pontos de recuperação manualmente

1. No AWS Backup console, no painel de navegação, escolha Backup vaults.
2. Na página Cofres de Backup, escolha o cofre no qual você armazenou os backups.
3. Escolha um ponto de recuperação, escolha o menu suspenso Ações e escolha Excluir.
4. 1. Se a sua lista contiver um backup contínuo, escolha uma das opções a seguir. Cada backup contínuo tem um único ponto de recuperação.
   - Excluir permanentemente meus dados de backup ou Excluir o ponto de recuperação. Ao selecionar uma dessas opções, você interromperá futuros backups contínuos e também excluirá seus dados de backup contínuo existentes.

     > **Note**
     >
     > Consulte Backups e point-in-time restauração contínuos (PITR) as considerações sobre backup contínuo do Amazon S3, Amazon RDS e Aurora.

   - Mantenha meus dados de backup contínuo ou desassocie o ponto de recuperação. Ao selecionar uma dessas opções, você interromperá futuros backups contínuos, mas reterá seus dados de backup contínuo existentes até que eles expirem, conforme definido pelo período de retenção.

     Um ponto de recuperação contínua (backup) não associado do Amazon S3 permanecerá em seu cofre de backup, mas seu estado será transferido para. `STOPPED`
   2. Para excluir todos os pontos de recuperação listados, digite excluir e escolha Excluir pontos de recuperação.
   3. AWS Backup começa a enviar seus pontos de recuperação para exclusão e exibe uma barra de progresso. Mantenha a guia do navegador aberta e não saia da página durante o processo de envio.
   4. Ao final do processo de envio, AWS Backup apresenta um status no banner. O status poderá ser:
      - Enviado com êxito. Você pode optar por Visualizar o progresso em relação ao status de exclusão de cada ponto de recuperação.
      - Falha ao enviar. Você pode optar por Visualizar o progresso em relação ao status de exclusão de cada ponto de recuperação ou Tentar novamente o envio.

- Um resultado misto em que alguns pontos de recuperação foram enviados com êxito, enquanto outros não foram enviados.

5. Se escolher Visualizar progresso, você poderá revisar o Status de exclusão de cada backup. Se um status de exclusão for Com falha ou Expirado, você poderá clicar nesse status para ver o motivo. Também é possível optar por Tentar novamente as exclusões com falha.

Solução de problemas de exclusões manuais

Em raras situações, AWS Backup pode não concluir sua solicitação de exclusão. AWS Backup usa a função vinculada ao serviço `AWSServiceRoleForBackup` para realizar exclusões.

Se houver falha na solicitação de exclusão, verifique se o perfil do IAM tem permissão para criar funções vinculadas a serviços. Especificamente, verifique se o perfil do IAM tem a ação `iam:CreateServiceLinkedRole`. Se não tiver, adicione essa permissão à função usada para criar um backup. Adicionar essa permissão permite AWS Backup realizar exclusões manuais.

Se, depois de confirmar que o perfil do IAM tem a ação `iam:CreateServiceLinkedRole`, seus pontos de recuperação ainda estiverem presos no status `DELETING`, provavelmente estamos investigando seu problema. Conclua a exclusão manual com as seguintes etapas:

1. Configure um lembrete para voltar em 2 a 3 dias.
2. Depois de dois a três dias, verifique se há pontos de exclusão recentes `EXPIRED` resultantes de sua primeira operação de exclusão manual.
3. Exclua manualmente esses pontos de recuperação `EXPIRED`.

Para obter mais informações, consulte Usar funções vinculadas a serviços e Adicionar e remover permissões de identidade do IAM.

Editar um backup

Depois de criar um backup usando AWS Backup, você pode alterar o ciclo de vida ou as tags do backup. O ciclo de vida define quando um backup é transferido para o armazenamento a frio e quando ele expira. O AWS Backup efetuará a transferência e a expiração de backups automaticamente de acordo com o ciclo de vida que você definir.

Para ver a lista de recursos que podem fazer a transição para o armazenamento frio, consulte a seção “Ciclo de vida até o armazenamento frio” da tabela Disponibilidade de recursos por recurso. A expressão de armazenamento frio é ignorada para outros recursos.

> **Note**
>
> A edição das tags de um backup usando o AWS Backup console só é suportada para backups dos sistemas de arquivos Amazon Elastic File System (Amazon EFS) e do Amazon DynamoDB avançado.
> As tags que foram adicionadas ao ponto de recuperação na criação de outros recursos ainda será exibidas, mas ficarão esmaecidas e não poderão ser editadas. Mesmo que essas tags não sejam editáveis no AWS Backup console, você pode editar as tags dos backups desses outros serviços usando o console ou a API do serviço.

Os backups transferidos para o armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias a mais do que a configuração de “número de dias para a transição para o armazenamento frio”. Quando você atualizar a configuração "número de dias para transferência ao armazenamento 'frio'", o valor deverá ser, no mínimo, a data de criação do backup mais um dia. A configuração de "número de dias para transferência ao armazenamento 'frio'" não poderá ser alterada depois que um backup for transferido para o armazenamento "frio".

Veja a seguir um exemplo de como atualizar o ciclo de vida de um backup.

Para editar o ciclo de vida de um backup

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Cofres de Backup.
3. Na seção Backups, selecione um backup.
4. Na página de detalhes do backup, selecione Editar.
5. Defina as configurações de ciclo de vida e escolha Salvar.

Restaurar um backup

Como restaurar

Para obter instruções de restauração do console e links para a documentação AWS Backup de cada tipo de recurso suportado, consulte os links na parte inferior desta página.

Para restaurar um backup de forma programática, use a operação StartRestoreJob da API.

Os valores de configuração (“restaurar metadados”) necessários para restaurar o recurso variam de acordo com o recurso que você deseja restaurar. Para obter os metadados de configuração com os quais seu backup foi criado, é possível chamar GetRecoveryPointRestoreMetadata. Exemplos de metadados de restauração também estão disponíveis nos links na parte inferior desta página.

A restauração a partir do armazenamento frio normalmente leva quatro horas a mais do que a restauração do armazenamento quente.

Para cada restauração, será criado um trabalho de restauração com um ID de trabalho exclusivo. Por exemplo, `1323657E-2AA4-1D94-2C48-5D7A423E7394`.

> **Note**
>
> AWS Backup não fornece nenhum contrato de nível de serviço (SLAs) para um período de restauração. Os tempos de restauração podem variar de acordo com a carga e a capacidade do sistema, mesmo para restaurações que contêm os mesmos recursos.

Restaurações não destrutivas

Quando você usa AWS Backup para restaurar um backup, ele cria um novo recurso com o backup que você está restaurando. Isso serve para proteger seus recursos existentes de serem destruídos pela atividade de restauração.

Testes de restauração

Você pode realizar testes nos recursos para simular uma experiência de restauração. Isso ajuda a determinar se você atende ao objetivo de tempo de restauração (RTO) organizacional e ajuda a se preparar para futuras necessidades de restauração.

Para obter mais informações, consulte Testes de restauração.

Copiar tags durante uma restauração

> **Note**
>
> As restaurações do Amazon DynamoDB, do Amazon S3 e do SAP HANA em instâncias do Amazon EC2, máquinas virtuais e recursos do Amazon Timestream não têm esse recurso disponível no momento.

Introdução

É possível pode copiar as tags ao restaurar um recurso se elas pertencerem ao recurso protegido no momento do backup. As tags, que são rótulos que contêm um par de chave/valor, podem ajudar você a identificar e pesquisar recursos. Ao iniciar um trabalho de restauração, as tags que pertenciam aos recursos originais de backup poderão ser adicionadas ao recurso que estiver sendo restaurado.

Ao optar por incluir tags durante um trabalho de restauração, essa etapa poderá substituir a sobrecarga e o trabalho de aplicar tags manualmente aos recursos após a conclusão de um trabalho de restauração. Observe que isso é diferente de adicionar novas tags aos recursos restaurados.

Ao restaurar um backup no fluxo do console, as tags de origem são copiadas por padrão. No console, desmarque a caixa se você quiser desativar a cópia de tags em um recurso restaurado

Na operação da API `StartRestoreJob`, o parâmetro `CopySourceTagsToRestoredResource` é definido como `false` por padrão, o que excluirá as tags de origem originais do recurso que você estiver restaurando. Se quiser incluir tags de origem originais, defina isso como `True`.

Considerações

- Um recurso pode ter até 50 tags, incluindo recursos restaurados. Consulte Como marcar seus AWS recursos para obter mais informações sobre limites de tags.
- Certifique-se de que as permissões corretas estejam presentes na função usada para restaurações de tags de cópia. A função padrão para restaurações contém as permissões necessárias. Uma função personalizada deve incluir permissões adicionais para marcar recursos.
- Atualmente, os seguintes recursos não são compatíveis com a inclusão da tag de restauração: VMware Cloud™ on AWS, VMware Cloud™ on AWS Outposts, sistemas locais, SAP HANA em instâncias do Amazon EC2, Timestream, DynamoDB, Advanced DynamoDB e Amazon S3.

- Para backups contínuos, as tags do recurso original a partir do backup mais recente serão copiadas no recurso restaurado.
- As tags não serão copiadas para restaurações em nível de item.
- As tags que foram adicionadas a um backup após a conclusão do trabalho de backup, mas que não estavam presentes no recurso original antes do backup, não serão copiadas no recurso restaurado. Somente os backups criados após 22 de maio de 2023 estão qualificados para cópia de tags na restauração.

Interação de tags com recursos específicos

- Amazon EC2
  - As tags aplicadas às instâncias restauradas do Amazon EC2 também são aplicadas aos volumes anexados restaurados do Amazon EBS.
  - As tags aplicadas aos volumes do EBS anexados às instâncias de origem não são copiadas para os volumes anexados às instâncias restauradas. Se você tiver políticas do IAM que permitem ou negam aos usuários o acesso aos volumes do EBS com base em suas tags, você deve reatribuir manualmente as tags necessárias aos volumes restaurados para garantir que suas políticas permaneçam em vigor.
- Quando você restaura um recurso do Amazon EFS, ele deve ser copiado em um novo sistema de arquivos. As restaurações em um sistema de arquivos existente não podem ter tags copiadas nele.
- Amazon RDS
  - Se o cluster do RDS do qual foi feito o backup ainda estiver ativo, as tags desse cluster serão copiadas.
  - Se o cluster original não estiver mais ativo, as tags do snapshot do cluster serão copiadas em vez disso.
  - As tags que estavam presentes no recurso no momento do backup serão copiadas durante a restauração, independentemente de o parâmetro booliano para `CopySourceTagsToRestoredResource` estar definido como `True` ou `False`. No entanto, se o snapshot não contiver tags, a configuração booliana acima será usada.
- Os clusters do Amazon Redshift, por padrão, sempre incluem tags durante um trabalho de restauração.

Copiar as tags pelo console

1. Abra o console do AWS Backup.
2. No painel de navegação, escolha Recursos protegidos e o ID do recurso do Amazon S3 que você deseja restaurar.
3. Na página Detalhes do recurso será exibida uma lista de pontos de recuperação para o ID de recurso selecionado. Como restaurar um recurso:

   a. No painel Backup, escolha o ID do ponto de recuperação do recurso.

   b. No canto superior direito do painel, escolha Restaurar (como alternativa, é possível acessar o cofre de backup, encontrar o ponto de recuperação e clicar em Ações e depois em Restaurar).
4. Na página Restaurar backup, localize o painel chamado Restaurar com tags. Para incluir todas as tags do recurso original, retenha a caixa de seleção (observe que no console essa caixa está marcada por padrão).
5. Clique em Restaurar backup depois de selecionar todas as configurações e funções preferidas.

Como incluir tags de forma programática

Use a operação de API `StartRestoreJob`. Certifique-se de que o seguinte parâmetro booliano esteja definido como `True`:

```
CopySourceTagsToRestoredResource = true
```

Se o parâmetro booliano `CopySourceTagsToRestoredResource` = `True`, o trabalho de restauração copiará as tags do(s) recurso(s) original(is) no material restaurado.

> **Important**
>
> O trabalho de restauração falhará se esse parâmetro for incluído em um recurso não suportado (VMware, sistemas locais, AWS Outposts SAP HANA em instâncias EC2, Timestream, DynamoDB, Advanced DynamoDB e 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
}
```

Solução de problemas de restauração de tags

ERRO: permissões insuficientes

SOLUÇÃO: certifique-se de ter as permissões necessárias em sua função de restauração para que possa incluir tags no recurso restaurado. A política padrão de função de serviço AWS gerenciado para restaurações AWSBackupServiceRolePolicyForRestores,, contém as permissões necessárias para essa tarefa.

Se você optar por usar uma função personalizada, verifique se as seguintes permissões estão presentes:

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

Para obter ter mais informações, consulte Permissões da API.

Status do trabalho de restauração

Você pode visualizar o status de um trabalho de restauração na página Trabalhos do console do AWS Backup . Os status dos trabalhos de restauração incluem: pendente, em execução, concluído, cancelado e com falha.

Tópicos

Restaurar dados do S3

Você pode restaurar os dados do S3 que você fez backup usando AWS Backup para a classe de armazenamento S3 Standard. É possível restaurar todos os objetos em um bucket ou objetos específicos. É possível restaurá-los em um bucket novo ou em um existente.

Permissões de restauração do Amazon S3

Antes de começar a restaurar os recursos, verifique se a função que você está usando tem permissões suficientes.

Para obter mais informações, consulte as seguintes entradas sobre políticas:

1. `AWSBackupServiceRolePolicyForS3Restore`
2. `AWSBackupServiceRolePolicyForRestores`
3. Políticas gerenciadas para AWS Backup

Considerações sobre restauração do Amazon S3

- AWS Backup cria um backup de todas as suas versões do S3, mas restaura somente a versão mais recente da pilha de versões em qualquer momento.
- As listas de controle de acesso (ACLs) devem estar habilitadas no bucket de destino, caso contrário, haverá falha no trabalho. Para habilitar as ACLs, siga as instruções na página Configurar ACLs.
- As restaurações de objetos serão ignoradas se o bucket de origem tiver um objeto com o mesmo nome ou ID de versão.
- Se restaurar objetos específicos, você poderá restaurar a versão atual de um objeto.
- Quando você restaura para o bucket S3 original,
  - AWS Backup não executa uma restauração destrutiva, o que significa que não AWS Backup colocará um objeto em um bucket no lugar de um objeto que já existe, independentemente da versão.
  - Um marcador de exclusão na versão atual é tratado como o objeto como inexistente, portanto, uma restauração pode ocorrer.
  - AWS Backup não exclui objetos (sem marcadores de exclusão) de um bucket durante uma restauração (exemplo: as chaves atualmente no bucket que não estavam presentes durante o backup permanecerão).
- Restauração de cópias entre regiões
  - Embora os backups do S3 possam ser copiados entre regiões, os trabalhos de restauração ocorrem somente na mesma região em que o backup ou a cópia original estão localizados.

    Example

    Exemplo: um bucket S3 criado na região Leste dos EUA (Norte da Virgínia) pode ser copiado para a região do Canadá (Central). O trabalho de restauração pode ser iniciado usando o bucket original na região Leste dos EUA (Norte da Virgínia) e restaurado nessa região, ou o trabalho de

restauração pode ser iniciado usando a cópia na região Canadá (Central) e restaurado nessa região.

- O método de criptografia original não pode ser usado para restaurar um ponto de recuperação (backup) copiado de outra região. A AWS KMS criptografia de cópia entre regiões não está disponível para os recursos do Amazon S3; em vez disso, use um tipo de criptografia diferente para um trabalho de restauração.

Use o AWS Backup console para restaurar os pontos de recuperação do Amazon S3

Para restaurar seus dados do Amazon S3 usando o AWS Backup console:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID do recurso do Amazon S3 que você deseja restaurar.
3. Na página Detalhes do recurso será exibida uma lista de pontos de recuperação para o ID de recurso selecionado. Como restaurar um recurso:

   a. No painel Backups, escolha o ID do ponto de recuperação do recurso.

   b. No canto superior direito do painel, escolha Restaurar.

      (Como alternativa, acesse o cofre de backup, encontre o ponto de recuperação e clique em Ações e depois em Restaurar.)
4. Se você estiver restaurando um backup contínuo, no painel Tempo de restauração, selecione uma das opções:

   a. Aceitar o padrão para restaurar para o horário restaurável mais recente.

   b. Especificar a data e a hora da restauração.
5. No painel Configurações, especifique se deseja restaurar o bucket inteiro ou realizar a restauração em nível do item.

   a. Se você escolher Restauração em nível de item, você restaura até 5 itens (objetos ou pastas em um bucket) por tarefa de restauração especificando o URI do S3 de cada item que identifica esse objeto de forma exclusiva.

      (Para obter mais informações sobre URIs do Amazon S3, consulte Métodos para acessar um bucket no Guia do usuário do Amazon Simple Storage Service.)

   b. Escolha Adicionar item para especificar outro item a ser restaurado.

6. Escolha seu destino de restauração. É possível restaurar no bucket de origem, usar o bucket existente ou criar um bucket.

   > **Note**
   >
   > Seu bucket de destino de restauração deve ter o controle de versão ativado. AWS Backup notificará você se o bucket selecionado não atender a esse requisito.

   a. Se você escolher Usar bucket existente, selecione o bucket S3 de destino no menu suspenso que mostra todos os buckets existentes na sua região atual. AWS

   b. Se escolher Criar um bucket, digite o nome do novo bucket. O novo bucket usará como padrão o versionamento do S3 ativado. As configurações de Block Public Access (BPA) serão desativadas por padrão. É possível modificar essas configurações após a criação do bucket no S3.

7. Para a criptografia de objetos em seu bucket do S3, você pode escolher a criptografia de objetos restaurados. Use chaves de criptografia originais (padrão), chave do Amazon S3 (SSE-S3) ou chave do AWS Key Management Service (SSE-KMS).

   Essas configurações se aplicam somente à criptografia dos objetos no bucket do S3. Isso não afeta a criptografia do próprio bucket.

   a. Usar chaves de criptografia originais (padrão) restaura objetos com as mesmas chaves de criptografia usadas pelo objeto de origem. Se um objeto de origem não estiver criptografado, esse método restaurará o objeto sem criptografia.

      Essa opção de restauração permite que você escolha opcionalmente uma chave de criptografia substituta para criptografar o (s) objeto (s) de restauração se a chave original não estiver disponível.

   b. Se escolher a chave do Amazon S3 (SSE-S3), não será necessário especificar nenhuma outra opção.

   c. Se você escolher a AWS Key Management Service chave (SSE-KMS), poderá fazer as seguintes escolhas: Chave gerenciada pela AWS (aws/s3), Escolher entre suas AWS KMS chaves ou Inserir ARN da chave. AWS KMS

      i. Se escolher Chave gerenciada pela AWS (aws/s3), não será necessário especificar nenhuma outra opção.

ii. Se você escolher entre suas AWS KMS chaves, selecione uma AWS KMS tecla no menu suspenso. Como alternativa, escolha Criar chave.

iii. Se você inserir o ARN da AWS KMS chave, digite o ARN na caixa de texto. Como alternativa, escolha Criar chave.

8. No painel de Restaurar perfil, escolha o perfil do IAM que o AWS Backup assumirá para essa restauração.
9. Escolha Restaurar backup. O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.

Use a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do Amazon S3

Usar `StartRestoreJob`. É possível especificar os seguintes metadados durante as restaurações do 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
```

Status do ponto de recuperação

Os pontos de recuperação terão um status indicando seu estado.

`PARTIAL`o status indica que não AWS Backup foi possível criar o ponto de recuperação antes que a janela de backup fosse fechada. Para aumentar a janela do seu plano de backup usando a API, consulte UpdateBackupPlan. Você também pode aumentar a janela do plano de backup usando o console, escolhendo e editando o plano de backup.

`EXPIRED`Do status indica que o ponto de recuperação excedeu seu período de retenção, mas AWS Backup não tem permissão ou não consegue excluí-lo. Para excluir manualmente esses pontos de recuperação, consulte Etapa 3: Excluir os pontos de recuperação na seção Limpar recursos da Introdução.

O status `STOPPED` ocorre em um backup contínuo em que um usuário executou alguma ação que faz com que o backup contínuo seja desativado. Isso pode ser causado pela remoção de permissões, pela desativação do controle de versão, pela desativação do envio de eventos para a Amazon EventBridge ou pela desativação das EventBridge regras estabelecidas pela. AWS Backup

Para resolver o status `STOPPED`, certifique-se de que todas as permissões solicitadas estejam em vigor e que o versionamento esteja habilitado no bucket do S3. Quando essas condições forem atendidas, a próxima instância de uma regra de backup em execução resultará na criação de um ponto de recuperação contínuo. Os pontos de recuperação com status PARADO não precisam ser excluídos.

Restaurando uma máquina virtual usando AWS Backup

Você pode restaurar uma máquina virtual no VMware, no VMware Cloud on, no VMware Cloud on AWS, em um volume do Amazon EBS ou em AWS Outposts uma instância do Amazon EC2. Restaurar (ou migrar) uma máquina virtual para o EC2 requer uma licença. Por padrão, AWS incluirá uma licença (cobranças aplicáveis). Para obter mais informações, consulte Opções de licenciamento no Guia do usuário do VM Import/Export.

Você pode restaurar uma máquina virtual VMware usando o AWS Backup console ou por meio do. AWS CLI Quando uma máquina virtual é restaurada, a pasta VMware Tools não é incluída. Consulte a documentação da VMware para reinstalar o VMware Tools.

AWS Backup as restaurações de máquinas virtuais não são destrutivas, ou seja, AWS Backup não substituem as máquinas virtuais existentes durante uma restauração. Em vez disso, o trabalho de restauração implanta uma nova máquina virtual.

Tarefas

- Considerações ao restaurar uma VM em uma instância do Amazon EC2
- Use o AWS Backup console para restaurar os pontos de recuperação da máquina virtual
- Use AWS CLI para restaurar pontos de recuperação de máquinas virtuais

Considerações ao restaurar uma VM em uma instância do Amazon EC2

- Restaurar (ou migrar) uma máquina virtual para o EC2 requer uma licença. Por padrão, um AWS incluirá uma licença (cobranças aplicáveis). Para obter mais informações, consulte Opções de licenciamento no Guia do usuário do VM Import/Export.
- Há um limite máximo de 5 TB (terabytes) para cada disco da máquina virtual.
- Você não pode especificar um par de chaves ao restaurar a máquina virtual em uma instância. Você pode adicionar um par de chaves `authorized_keys` durante a execução (por meio de dados do usuário da instância) ou após a execução (conforme descrito nesta seção de solução de problemas no Guia do usuário do Amazon EC2).
- Confirme se seu sistema operacional tem suporte para importação e exportação do Amazon EC2 no Guia do usuário do VM Import/Export.
- Analise as limitações envolvidas na importação de VMs para o Amazon EC2 no Guia do usuário do VM Import/Export.
- Ao restaurar para uma instância do Amazon EC2 usando AWS CLI, você deve especificar. `"RestoreTo":"EC2Instance"` Todos os outros atributos têm valores padrão.

Use o AWS Backup console para restaurar os pontos de recuperação da máquina virtual

Você pode restaurar uma máquina virtual de vários locais no painel de navegação esquerdo do AWS Backup console:

- Escolha Hipervisores para visualizar os pontos de recuperação de máquinas virtuais gerenciadas por um hipervisor conectado ao AWS Backup.
- Escolha Máquinas virtuais para visualizar os pontos de recuperação de máquinas virtuais em todos os seus hipervisores conectados ao AWS Backup.
- Escolha Cofres de backup para ver os pontos de recuperação armazenados em um cofre específico AWS Backup .
- Escolha Recursos protegidos para visualizar os pontos de recuperação em todos os seus recursos AWS Backup protegidos.

Se precisar restaurar uma máquina virtual que não tenha mais uma conexão com o gateway de backup, escolha Cofres de backup ou Recursos protegidos para localizar seu ponto de recuperação.

Opções

- Restauração para VMware
- Restaurar em um volume do Amazon EBS
- Restaurar em uma instância do Amazon EC2

Para restaurar uma máquina virtual para VMware, VMware Cloud on e VMware Cloud on AWSAWS Outposts

1. Nas visualizações de hipervisores ou de máquinas virtuais, escolha o nome da VM a ser restaurada. Na visualização Recursos protegidos, escolha o ID do recurso da máquina virtual a ser restaurada.
2. Escolha o botão radial ao lado do ID do ponto de recuperação a ser restaurado.
3. Escolha Restore.
4. Selecione o Tipo de recuperação.

    a. A restauração completa restaura todos os discos da máquina virtual.

    b. A restauração em nível de disco restaura uma seleção definida pelo usuário de um ou mais discos. Use o menu suspenso para selecionar quais discos restaurar.
5. Escolha o Local de restauração. As opções são VMware, VMware Cloud on e VMware Cloud on AWS. AWS Outposts
6. Se você estiver fazendo uma restauração completa, prossiga para a próxima etapa. Se você estiver executando uma restauração em nível de disco, haverá um menu suspenso em Discos da VM. Escolha um ou mais volumes inicializáveis a serem restaurados.
7. Selecionar um hipervisor no menu suspenso para gerenciar a máquina virtual restaurada
8. Para a máquina virtual restaurada, use as práticas recomendadas de máquina virtual da sua organização para especificar os seguintes itens:

    a. Nome

    b. Caminho (como `/datacenter/vm`)

    c. Nome do recurso de computação (como VMHost ou Cluster)

    Se um host fizer parte de um cluster, não será possível restaurar para o host, somente para o cluster fornecido.

    d. Datastore

9. Em Função de restauração, selecione a função padrão (recomendada) ou Escolher um perfil do IAM usando o menu suspenso.
10. Escolha Restaurar backup.
11. Opcional: verifique quando o trabalho de restauração tem o status `Completed`. No painel de navegação esquerdo, escolha Trabalhos.

Para restaurar uma máquina virtual em um volume do Amazon EBS

1. Nas visualizações de hipervisores ou de máquinas virtuais, escolha o nome da VM a ser restaurada. Na visualização Recursos protegidos, escolha o ID do recurso da máquina virtual a ser restaurada.
2. Escolha o botão radial ao lado do ID do ponto de recuperação a ser restaurado.
3. Escolha Restore.
4. Selecione o Tipo de recuperação.
    - A restauração de disco restaura uma seleção definida pelo usuário de um disco. Use o menu suspenso para selecionar qual disco restaurar.
5. Escolha o Local de restauração como Amazon EBS.
6. No menu suspenso Disco da VM, escolha o volume inicializável a ser restaurado.
7. Em Tipo de volume, escolha o tipo de volume.
8. Escolha sua zona de disponibilidade.
9. Criptografia (opcional). Marque a caixa se você optar por criptografar o volume do EBS.
10. Selecione sua chave KMS no menu.
11. Em Restaurar função, selecione a função padrão (recomendada) ou Escolha uma função do IAM.
12. Escolha Restaurar backup.
13. Opcional: verifique quando o trabalho de restauração tem o status `Completed`. No painel de navegação esquerdo, escolha Trabalhos.
14. Opcional: acesse Como criar um volume lógico LVM em todo um volume do Amazon EBS? para saber mais sobre como montar volumes gerenciados e acessar dados no volume restaurado do Amazon EBS.

Para restaurar uma máquina virtual em uma instância do Amazon EC2

1. Nas visualizações de hipervisores ou de máquinas virtuais, escolha o nome da VM a ser restaurada. Na visualização Recursos protegidos, escolha o ID do recurso da máquina virtual a ser restaurada.
2. Escolha o botão radial ao lado do ID do ponto de recuperação a ser restaurado.
3. Escolha Restore.
4. Selecione o Tipo de recuperação.
   - A restauração completa restaura completamente o sistema de arquivos, incluindo a pasta e os arquivos no nível raiz.
5. Escolha o Local de restauração como Amazon EC2.
6. Em Tipo de instância, escolha a combinação de computação e memória necessária para executar seu aplicativo na nova instância.

   > **Tip**
   >
   > Escolha um tipo de instância que corresponda ou exceda as especificações da máquina virtual original. Para obter mais informações, consulte o Guia de tipos de instância do Amazon EC2.

7. Para Virtual Private Cloud (VPC), escolha uma nuvem privada virtual (VPC), que define o ambiente de rede para a instância.
8. Em Subnet, escolha uma das sub-redes na VPC. Sua instância recebe um endereço IP privado do intervalo de endereços da sub-rede.
9. Para grupos de segurança, escolha um grupo de segurança, que atua como um firewall para o tráfego para sua instância.
10. Em Restaurar função, selecione a função padrão (recomendada) ou Escolha uma função do IAM.
11. Opcional: para executar um script em sua instância na inicialização, expanda Configurações avançadas e insira o script em Dados do usuário.
12. Escolha Restaurar backup.
13. Opcional: verifique quando o trabalho de restauração tem o status `Completed`. No painel de navegação esquerdo, escolha Trabalhos.

Use AWS CLI para restaurar pontos de recuperação de máquinas virtuais

Usar `StartRestoreJob`.

Você pode especificar os seguintes metadados para a restauração de uma máquina virtual no Amazon EC2 e no Amazon EBS:

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

Você pode especificar os seguintes metadados para uma restauração de máquina virtual para VMware, VMware Cloud on e VMware cloud on AWS Outpost: AWS

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

Este exemplo mostra como realizar uma restauração completa para a 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"}'
```

Restaurar um sistema de arquivos do FSX

As opções de restauração que estão disponíveis quando você usa AWS Backup para restaurar sistemas de arquivos Amazon FSx são as mesmas do backup nativo do Amazon FSx. Você pode usar o ponto de recuperação de um backup para criar um novo sistema de arquivos e restaurar um point-in-time instantâneo de outro sistema de arquivos.

Ao restaurar os sistemas de arquivos Amazon FSx AWS Backup , cria um novo sistema de arquivos e o preenche com os dados (o Amazon FSx NetApp for ONTAP permite restaurar um volume em um sistema de arquivos existente). Isso é semelhante à forma como o Amazon FSx nativo faz backup e restaura sistemas de arquivos. Restaurar um backup em um novo sistema de arquivos leva o mesmo tempo que criar um sistema de arquivos. Os dados restaurados do backup são carregados lentamente no sistema de arquivos. Portanto, você pode experimentar uma latência um pouco maior durante o processo.

> **Note**
>
> Não é possível restaurar para um sistema de arquivos do Amazon FSx existente e não é possível restaurar arquivos ou pastas individuais.
> O FSx para ONTAP não é compatível com o backup de determinados tipos de volume, incluindo volumes de DP (proteção de dados), volumes de LS (compartilhamento de carga), volumes completos ou volumes em sistemas de arquivos que estão cheios. Para ter mais informações, consulte FSx para ONTAP – trabalhar com backups.
> AWS Backup cofres que contêm pontos de recuperação dos sistemas de arquivos Amazon FSx são visíveis do lado de fora. AWS BackupÉ possível restaurar os pontos de recuperação usando o Amazon FSx, mas não é possível excluí-los.

Você pode ver os backups criados pela funcionalidade de backup automático integrada do Amazon FSx no AWS Backup console. Você também pode recuperar esses backups usando AWS Backup

o. No entanto, você não pode excluir esses backups nem alterar as programações de backup automático dos seus sistemas de arquivos Amazon FSx usando. AWS Backup

Você pode restaurar os backups criados AWS Backup usando o AWS Backup console, a API ou AWS CLI. Esta seção mostra como usar o AWS Backup console para restaurar sistemas de arquivos Amazon FSx.

Use o AWS Backup console para restaurar os pontos de recuperação do Amazon FSx

Restaurar um sistema de arquivos do FSx para Windows File Server

Como restaurar um sistema de arquivos do FSx para Windows File Server

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID do recurso do Amazon FSx que você deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Escolha o ID do ponto de recuperação do recurso.
4. No canto superior direito do painel, escolha Restaurar para abrir a página Restaurar backup.
5. Na seção Detalhes do sistema de arquivos, o ID do seu backup é exibida em ID do backup e o tipo de sistema de arquivos é exibido em Tipo de sistema de arquivos. É possível restaurar os sistemas de arquivos do FSx para Windows File Server e do FSx para Lustre.
6. Em Tipo de implantação, aceite o padrão. Não é possível alterar o tipo de implantação de um sistema de arquivos durante a restauração.
7. Escolha o Tipo de armazenamento a ser usado. Se a capacidade de armazenamento do seu sistema de arquivos for inferior a 2.000 GiB, não será possível usar o tipo de armazenamento HDD.
8. Em Capacidade de throughput, escolha Capacidade de throughput recomendada para usar a taxa recomendada de 16 MB por segundo (MBps) ou escolha Especificar capacidade de throughput e insira uma nova taxa.
9. Na seção Rede e segurança, forneça as informações necessárias.
10. Se você estiver restaurando um sistema de arquivos do FSx para Windows File Server, forneça as informações de autenticação do Windows usadas para acessar o sistema de arquivos ou crie um sistema de arquivos.

> **Note**
>
> Ao restaurar um backup, não é possível alterar o tipo de Active Directory no sistema de arquivos.

Para obter mais informações sobre o Microsoft Active Directory, consulte Trabalhar com o Active Directory no Amazon FSx para Windows File Server no Guia do usuário do Amazon FSx para Windows File Server.

11. (Opcional) Na seção Backup e manutenção, forneça as informações para definir suas preferências de backup.
12. Na seção Função de restauração, escolha o perfil do IAM que o AWS Backup usará para criar e gerenciar os backups em seu nome. Recomendamos que você escolha a Função padrão. Se não houver nenhuma função padrão, será criada uma para você com as permissões corretas. Você também pode fornecer seu próprio perfil do IAM.
13. Verifique todas as entradas e escolha Restaurar backup.

Restaurar um sistema de arquivos do Amazon FSx para Lustre

AWS Backup suporta sistemas de arquivos Amazon FSx for Lustre que têm um tipo de implantação de armazenamento persistente e não estão vinculados a um repositório de dados como o Amazon S3.

Como restaurar um sistema de arquivos do Amazon FSx para Lustre

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID do recurso do Amazon FSx que você deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Escolha o ID do ponto de recuperação do recurso.
4. No canto superior direito do painel, escolha Restaurar para abrir a página Restaurar backup para o novo sistema de arquivos.
5. Na seção Configurações, o ID do seu backup é exibido em ID do backup e o tipo de sistema de arquivos é exibido em Tipo de sistema de arquivos. O tipo de sistema de arquivos deve ser Lustre.

6. (Opcional) Insira um nome para o sistema de arquivos.
7. Escolha um tipo de implantação. AWS Backup suporta apenas o tipo de implantação persistente. Não é possível alterar o tipo de implantação de um sistema de arquivos durante a restauração.

   O tipo de implantação persistente é para armazenamento de longo prazo. Para obter informações detalhadas sobre as opções de implantação do FSx para Lustre, consulte Usar as opções de implantação disponíveis para sistemas de arquivos do Amazon FSx para Lustre no Guia do usuário do Amazon FSx para Lustre.
8. Escolha a taxa de throughput por unidade de armazenamento que você deseja usar.
9. Especifique a capacidade de armazenamento a ser usada. Insira uma capacidade entre 32 GiB e 64,436 GiB.
10. Na seção Rede e segurança, forneça as informações necessárias.
11. (Opcional) Na seção Backup e manutenção, forneça as informações para definir suas preferências de backup.
12. Na seção Função de restauração, escolha o perfil do IAM que o AWS Backup usará para criar e gerenciar os backups em seu nome. Recomendamos que você escolha a Função padrão. Se não houver nenhuma função padrão, será criada uma para você com as permissões corretas. Você também pode fornecer seu perfil do IAM.
13. Verifique todas as entradas e escolha Restaurar backup.

Restauração de volumes Amazon FSx NetApp para ONTAP

Para restaurar volumes do Amazon FSx para NetApp ONTAP:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID do recurso do Amazon FSx que você deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Escolha o ID do ponto de recuperação do recurso.
4. No canto superior direito do painel, escolha Restaurar para abrir a página Restaurar.

   A primeira seção, Detalhes do sistema de arquivos, exibe o ID do ponto de recuperação, o ID do sistema de arquivos e o tipo do sistema de arquivos.
5. Em Opções de restauração, há várias seleções. Primeiro, escolha o Sistema de arquivos no menu suspenso.

6. Em seguida, escolha a Máquina virtual de armazenamento preferida no menu suspenso.
7. Insira um nome para o volume.
8. Especifique o Caminho da junção, que é o local em seu sistema de arquivos onde seu volume será montado.
9. Especifique o Tamanho do volume em megabytes (MB) que você está criando.
10. (Opcional) Você pode optar por Habilitar eficiência de armazenamento marcando a caixa. Isso permitirá desduplicação, a compressão e a compactação.
11. No menu suspenso Política de camadas do grupo de capacidade, selecione a preferência de camadas.
12. Nas permissões de restauração, escolha a função do IAM que AWS Backup será usada para restaurar os backups.
13. Verifique todas as entradas e escolha Restaurar backup.

Restaurar um sistema de arquivos do Amazon FSx para OpenZFS

Como restaurar um sistema de arquivos do FSx para OpenZFS:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID do recurso do Amazon FSx que você deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Escolha o ID do ponto de recuperação do recurso.
4. No canto superior direito do painel, escolha Restaurar para abrir a página Restaurar backup.

   Na seção Detalhes do sistema de arquivos, o ID do seu backup é exibida em ID do backup e o tipo de sistema de arquivos é exibido em Tipo de sistema de arquivos. O tipo de sistema de arquivos deve ser FSx para OpenZFS.
5. Em Opções de restauração, é possível selecionar Restauração rápida ou Restauração padrão. A restauração rápida usará as configurações padrão do sistema de arquivos de origem. Se você estiver fazendo a Restauração rápida, prossiga para a Etapa 7.

   Se escolher Restauração padrão, especifique as seguintes configurações adicionais:

   a. IOPS de SSD provisionado: escolha o botão de opção Automático ou escolha a opção Provisionado pelo usuário, se disponível.

b. Capacidade de throughput: escolha a capacidade de throughput recomendada de 64 MB/s ou opte por Especificar a capacidade de throughput.

c. (Opcional) Grupos de segurança da VPC: especifique grupos de segurança da VPC para associar à interface de rede do seu sistema de arquivos.

d. Chave de criptografia: especifique a AWS Key Management Service chave para proteger os dados restaurados do sistema de arquivos em repouso.

e. (Opcional) Configuração do volume raiz: essa configuração está recolhida por padrão. Expanda-a clicando no circunflexo (seta) apontando para baixo. A criação de um sistema de arquivos a partir de um backup criará um sistema de arquivos. Os volumes e os snapshots manterão suas configurações de origem.

f. (Opcional) Backup e manutenção: para definir um backup programado, clique no circunflexo (seta) apontando para baixo para expandir a seção. Você pode escolher a janela de backup, a hora e o minuto, o período de retenção e a janela de manutenção semanal.

6. (Opcional) É possível inserir um nome para o volume.
7. A capacidade de armazenamento SSD exibirá a capacidade de armazenamento do sistema de arquivos.
8. Escolha a Nuvem privada virtual (VPC) a partir da qual seu sistema de arquivos pode ser acessado.
9. No menu suspenso Sub-rede, escolha a sub-rede na qual a interface de rede do sistema de arquivos reside.
10. Na seção Restaurar função, escolha a função do IAM que AWS Backup será usada para criar e gerenciar seus backups em seu nome. Recomendamos que você escolha a Função padrão. Se não houver nenhuma função padrão, será criada uma para você com as permissões corretas. Também é possível optar por utilizar um perfil do IAM.
11. Verifique todas as entradas e escolha Restaurar backup.

Use a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do Amazon FSx

Para restaurar o Amazon FSx usando a API ou a CLI, use `StartRestoreJob`. É possível especificar os seguintes metadados durante qualquer restauração do Amazon FSx:

```
FileSystemId
FileSystemType
```

```
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

Metadados de restauração do FSx para Windows File Server

É possível especificar os seguintes metadados durante uma restauração do FSx para Windows File Server:

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

Metadados de restauração do FSx para Lustre

É possível especificar `PerUnitStorageThroughput` e `DriveCacheType` durante uma restauração do FSx para Lustre.

Metadados de restauração do FSx para ONTAP

É possível especificar os seguintes metadados durante uma restauração do FSx para ONTAP:

- Nome #name do volume a ser criado
- OntapConfiguration: # configuração do botão
- `junctionPath`
- `sizeInMegabytes`

- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

Metadados de restauração do FSx para OpenZFS

É possível especificar os seguintes metadados durante uma restauração do FSx para OpenZFS:

- `ThroughputCapacity`
- `DesklopsConfiguration`
- Se Iops for especificado, você deverá incluir um valor entre 0 e 160.000, mas não inclua Modo.

Exemplo de comando de restauração da 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\"}"'
```

Exemplo de metadados de restauração:

```
"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\\\"]\"}"
```

Restaurar um volume do Amazon EBS

Quando você restaura um snapshot do Amazon Elastic Block Store (Amazon EBS), AWS Backup cria um novo volume do Amazon EBS que você pode anexar à sua instância do Amazon EC2.

É possível optar por restaurar o snapshot como um volume do EBS ou como um volume do AWS Storage Gateway .

Use o AWS Backup console para restaurar os pontos de recuperação do Amazon EBS

Como restaurar um volume do Amazon EBS

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID de recurso do EBS que deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Para restaurar um recurso, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.
4. Especifique os parâmetros de restauração para o recurso. Os parâmetros de restauração inseridos são específicos do tipo de recurso selecionado.

   Em Tipo de recurso, escolha o AWS recurso a ser criado ao restaurar esse backup.
5. Se você escolher Volume do EBS, forneça os valores para o Tipo de volume, Tamanho (GiB) e escolha uma Zona de disponibilidade.

   - Depois de Throughput, haverá uma caixa de seleção opcional Criptografar esse volume. Essa opção permanecerá ativa se o ponto de recuperação do EBS estiver criptografado.

     Você pode especificar uma chave KMS ou criar uma AWS KMS chave.

   Se você escolher o volume do Storage Gateway, escolha um Gateway em um estado acessível. Escolha também o Nome do destino iSCSI.

   - Para gateways de Volume armazenado, escolha um ID de disco.
   - Em gateways de volume em cache, escolha uma capacidade que seja pelo menos tão grande quanto a do recurso protegido.
6. Para a função Restaurar, escolha a função do IAM que AWS Backup será assumida para essa restauração.

> **Note**
>
> Se a função AWS Backup padrão não estiver presente na sua conta, uma função padrão será criada para você com as permissões corretas. Você poderá excluir essa função padrão ou torná-la inutilizável.

7. Escolha Restaurar backup.

   O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.

A restauração de um snapshot arquivado do EBS o move temporariamente do armazenamento frio para o armazenamento quente a fim de criar um novo volume do EBS. Esse tipo de restauração incorre em uma cobrança única de recuperação. Os custos dos armazenamentos quente e frio são cobrados durante esse período de restauração. Os volumes do EBS em armazenamento refrigerado não podem ser restaurados em um volume de gateway de Backup.

Você pode restaurar um snapshot arquivado do EBS no armazenamento frio usando o console do AWS Backup ou a linha de comandos. A restauração do armazenamento frio pode levar até 72 horas. Para obter mais informações, consulte Arquivar snapshots do Amazon EBS no Guia do usuário do Amazon EC2.

Console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Navegue até Cofres de backup > *Cofre* > Restaurar o snapshot arquivado do EBS.
3. Na seção Configurações, insira um valor de 0 a 180, ambos incluídos, que especifique o número de dias para restaurar temporariamente um snapshot arquivado.
4. Insira outras configurações: tipo de volume, tamanho, IOPS, zona de disponibilidade, throughput e criptografia.
5. Escolha um Perfil de restauração.
6. Selecione Restaurar backup. No pop-up de confirmação, confirme os snapshots e o tipo de restauração. Depois, selecione Restaurar snapshot.

AWS CLI

1. Usar o `start-restore-job`
2. Inclua os parâmetros.
3.
4.
5.

Use a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do Amazon EBS

Para restaurar o Amazon EBS usando a API ou a CLI, use `StartRestoreJob`. É possível especificar os seguintes metadados durante qualquer restauração do 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
```

Exemplo:

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

Restaurar um sistema de arquivos do Amazon EFS

Se estiver restaurando uma instância do Amazon Elastic File System (Amazon EFS), você poderá executar uma restauração completa ou uma restauração em nível de item.

Restauração completa

Quando você executa uma restauração completa, todo o sistema de arquivos é restaurado.

AWS Backup não oferece suporte a restaurações destrutivas com o Amazon EFS. Uma restauração destrutiva ocorre quando um sistema de arquivos restaurado exclui ou substitui o sistema de arquivos de origem ou existente. Em vez disso, o AWS Backup restaura o sistema de arquivos em um diretório de recuperação fora do diretório raiz.

Restauração em nível de item

Quando você executa uma restauração em nível de item, AWS Backup restaura um arquivo ou diretório específico. Você deve especificar o caminho relativo à raiz do sistema de arquivos. Por exemplo, se o sistema de arquivos estiver montado em `/user/home/myname/efs` e o caminho do arquivo for `user/home/myname/efs/file1`, insira **`/file1`**. Os caminhos diferenciam letras maiúsculas de minúsculas. Caracteres curinga e strings de regex não são compatíveis. Seu caminho pode ser diferente do que está no host se o sistema de arquivos for montado usando um ponto de acesso.

É possível selecionar até 10 itens quando usar o console para executar uma restauração do EFS. Não há limite de itens quando você usa a CLI para restaurar. No entanto, há um limite de 200 KB no tamanho dos metadados de restauração que podem ser transmitidos.

Você pode restaurar esses itens para um sistema de arquivos novo ou existente. De qualquer forma, o AWS Backup cria um novo diretório do Amazon EFS (`aws-backup-restore_`*`datetime`*) fora do diretório raiz para conter os itens. A hierarquia completa dos itens especificados é preservada no diretório de recuperação. Por exemplo, se o diretório A contiver os subdiretórios B, C e D, o AWS Backup manterá a estrutura hierárquica quando A, B, C e D forem recuperados. Independentemente de você executar uma restauração em nível de item do Amazon EFS para um sistema de arquivos existente ou para um novo sistema de arquivos, cada tentativa de restauração criará um novo diretório de recuperação fora do diretório raiz para conter os arquivos restaurados. Se você tentar várias restaurações para o mesmo caminho, poderão existir vários diretórios contendo os itens restaurados.

> **Note**
>
> Se você mantiver apenas um backup semanal, só será possível restaurar para o estado do sistema de arquivos no momento em que o backup foi feito. Não será possível restaurar backups incrementais anteriores.

Use o AWS Backup console para restaurar um ponto de recuperação do Amazon EFS

Como restaurar um sistema de arquivos do Amazon EFS

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Seu cofre de backup do EFS recebe a política de acesso Deny `backup:StartRestoreJob` após a criação. Se estiver restaurando o cofre de backup pela primeira vez, você deverá alterar a política de acesso da seguinte maneira:

   a. Escolha Cofres de backup.

   b. Escolha o cofre de backup que contém o ponto de recuperação que você deseja restaurar.

   c. Role para baixo até a Política de acesso do cofre

   d. Se presente, exclua `backup:StartRestoreJob` da `Statement`. Faça isso escolhendo Editar, excluindo `backup:StartRestoreJob` e escolhendo Salvar política.
3. No painel de navegação, escolha Recursos protegidos e o ID do sistema de arquivos do EFS que deseja restaurar.
4. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID do sistema de arquivos selecionado. Para restaurar um sistema de arquivos, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do sistema de arquivos. No canto superior direito do painel, escolha Restaurar.
5. Especifique os parâmetros de restauração para o sistema de arquivos. Os parâmetros de restauração inseridos são específicos do tipo de recurso selecionado.

   É possível executar uma Restauração completa, que restaura todo o sistema de arquivos. Ou, poderá restaurar arquivos e diretórios específicos usando a Restauração em nível de item.

   - Escolha a opção Restauração completa para restaurar o sistema de arquivos inteiro, incluindo todas as pastas e arquivos de nível raiz.
   - Escolha a opção de Restauração em nível de item para restaurar um arquivo ou diretório específico. É possível selecionar e restaurar até cinco itens dentro do seu Amazon EFS.

     Para restaurar um arquivo ou diretório específico, é necessário especificar o caminho relativo relacionado ao ponto de montagem. Por exemplo, se o sistema de arquivos estiver montado em `/user/home/myname/efs` e o caminho do arquivo for `user/home/myname/efs/file1`, insira **`/file1`**. Os caminhos diferenciam maiúsculas e minúsculas e não podem conter caracteres especiais, curingas e strings regex.

1. Na caixa de texto Caminho do item insira o caminho do arquivo ou pasta.
2. Escolha Adicionar item para adicionar arquivos ou diretórios adicionais. É possível selecionar e restaurar até cinco itens no sistema de arquivos do EFS.

6. Para Restaurar local

   - Escolha a opção Restaurar para o diretório no sistema de arquivos de origem se desejar restaurar para o sistema de arquivos de origem.
   - Escolha a opção Restaurar para um novo sistema de arquivos se desejar restaurar para um sistema de arquivos diferente.

7. Em Tipo do sistema de arquivos

   - (Recomendado) Escolha Regional se quiser restaurar seu sistema de arquivos em várias zonas de AWS disponibilidade.
   - Escolha Uma zona se quiser restaurar o sistema de arquivos em uma única zona de disponibilidade. Em seguida, no menu suspenso Zona de disponibilidade, escolha o destino para a restauração.

   Para obter mais informações, consulte Gerenciar classes de armazenamento do Amazon EFS no Guia do usuário do Amazon EFS.

8. Em Performance

   - Se você optar por realizar uma restauração regional, escolha Uso geral (recomendado) ou E/S máx.
   - Se optar por realizar uma restauração em uma zona, você deverá escolher Uso geral (recomendado). As restaurações de uma zona não são compatíveis com E/S máx.

9. Em Habilitar criptografia

   - Escolha Ativar criptografia, se desejar criptografar seu sistema de arquivos. Os IDs e aliases da chave KMS aparecem na lista depois de serem criados usando o console AWS Key Management Service (AWS KMS).
   - Na caixa de texto Chave do KMS, escolha a chave que deseja usar na lista.

10. Para a função Restaurar, escolha a função do IAM que AWS Backup será assumida para essa restauração.

> **Note**
>
> Se a função AWS Backup padrão não estiver presente na sua conta, uma função padrão será criada para você com as permissões corretas. Você poderá excluir essa função padrão ou torná-la inutilizável.

11. Escolha Restaurar backup.

    O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.

> **Note**
>
> Se você mantiver apenas um backup semanal, só será possível restaurar para o estado do sistema de arquivos no momento em que o backup foi feito. Não será possível restaurar backups incrementais anteriores.

Use a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do Amazon EFS

Usar `StartRestoreJob`. Ao restaurar uma instância do Amazon EFS, você pode restaurar um sistema de arquivos inteiro ou arquivos ou diretórios específicos. Para restaurar recursos do Amazon EFS, você precisará das seguintes informações:

- `file-system-id`— O ID do sistema de arquivos Amazon EFS que é copiado pelo AWS Backup. Restaurado em `GetRecoveryPointRestoreMetadata`. Isso não é necessário quando um novo sistema de arquivos é restaurado (esse valor é ignorado se o parâmetro `newFileSystem` for`True`).
- `Encrypted`: um valor booliano que, quando verdadeiro, especifica que o sistema de arquivos foi criptografado. Se `KmsKeyId` for especificado, `Encrypted` deverá ser definido como `true`.
- `KmsKeyId`— Especifica a AWS KMS chave usada para criptografar o sistema de arquivos restaurado.
- `PerformanceMode`: especifica o modo de throughput do sistema de arquivos.
- `CreationToken`: um valor fornecido pelo usuário que garante a exclusividade (idempotência) da solicitação.

- `newFileSystem`: um valor booliano que, quando verdadeiro, especifica que o ponto de recuperação foi restaurado para um novo sistema de arquivos do Amazon EFS.
- `ItemsToRestore` : uma matriz de até cinco strings em que cada string é um caminho de arquivo. Use `ItemsToRestore` para restaurar arquivos ou diretórios específicos, em vez de todo o sistema de arquivos. Esse parâmetro é opcional.

Você também pode incluir `aws:backup:request-id`.

As restaurações de uma zona podem ser realizadas incluindo parâmetros:

```
"singleAzFilesystem": "true"
"availabilityZoneName": "ap-northeast-3"
```

Para obter mais informações sobre os valores de configuração do Amazon EFS, consulte create-file-system.

Desabilitar backups automáticos no Amazon EFS

Por padrão, o Amazon EFS cria backups de dados automaticamente. Esses backups são representados como pontos de recuperação em AWS Backup. As tentativas de remover o ponto de recuperação resultarão em uma mensagem de erro informando que não há privilégios suficientes para realizar a ação.

É uma melhor prática manter esse backup automático ativo. Especialmente no caso de exclusão acidental de dados, esse backup permite a restauração do conteúdo do sistema de arquivos até a data do último ponto de recuperação criado.

No caso improvável de você desejar desativá-los, a política de acesso deve ser alterada de `"Effect": "Deny"` para `"Effect": "Allow"`. Consulte o Guia do usuário do Amazon EFS para obter mais informações sobre como ativar ou desativar backups automáticos.

Restaurar uma tabela do Amazon DynamoDB

Use o AWS Backup console para restaurar os pontos de recuperação do DynamoDB

Como restaurar uma tabela do DynamoDB

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.

2. No painel de navegação, escolha Recursos protegidos e o ID do recurso do DynamoDB que deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Para restaurar um recurso, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.
4. Para Configurações, campo de texto Novo nome de tabela, insira um novo nome de tabela.
5. Para a função Restaurar, escolha a função do IAM que AWS Backup será assumida para essa restauração.
6. Em Configurações de criptografia:

   a. Se seu backup for gerenciado pelo DynamoDB (seu ARN começa `arn:aws:dynamodb` com) AWS Backup , criptografa sua tabela restaurada usando uma chave própria. AWS

      Para escolher uma chave diferente para criptografar sua tabela restaurada, você pode usar a AWS Backup StartRestoreJoboperação ou realizar a restauração no console do DynamoDB.

   b. Se seu backup suportar AWS Backup gerenciamento total (seu ARN começa com`arn:aws:backup`), você pode escolher qualquer uma das seguintes opções de criptografia para proteger sua tabela restaurada:

      - (Padrão) Chave do KMS de propriedade do DynamoDB (sem cobrança adicional pela criptografia)
      - Chave do KMS gerenciada pelo DynamoDB (cobranças do KMS aplicáveis)
      - Chave do KMS gerenciada pelo cliente (cobranças do KMS aplicáveis)

      As chaves “de propriedade do DynamoDB” e “gerenciadas pelo DynamoDB” são iguais às chaves “de propriedade da AWS” e “gerenciada pela AWS”, respectivamente. Para obter esclarecimentos, consulte Criptografia em repouso: como funciona no Guia do desenvolvedor do Amazon DynamoDB.

      Para obter mais informações sobre o AWS Backup gerenciamento completo, consulteBackup avançado do DynamoDB.

> **Note**
>
> A orientação a seguir se aplica somente se você restaurar um backup copiado E quiser criptografar a tabela restaurada com a mesma chave usada para criptografar a tabela original.
> Ao restaurar um backup entre regiões, para criptografar sua tabela restaurada usando a mesma chave que você usou para criptografar sua tabela original, sua chave deve ser uma chave multirregional. AWS-chaves próprias e AWS gerenciadas não são chaves multirregionais. Para obter mais informações, consulte Chaves multirregiões, no Guia do desenvolvedor do AWS Key Management Service .
> Ao restaurar um backup entre contas, para criptografar sua tabela restaurada usando a mesma chave que você usou para criptografar sua tabela original, você deve compartilhar a chave em sua conta de origem com sua conta de destino. AWS chaves próprias e AWS gerenciadas não podem ser compartilhadas entre contas. Para obter mais informações, consulte Permitir que usuários em outras contas usem uma chave do KMS no Guia do desenvolvedor do AWS Key Management Service .

7. Escolha Restaurar backup.

   O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.

Use a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do DynamoDB

Usar `StartRestoreJob`. É possível especificar os seguintes metadados durante qualquer restauração do DynamoDB: Os metadados não diferenciam maiúsculas de minúsculas.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

Veja a seguir um exemplo do argumento `restoreMetadata` para uma operação `StartRestoreJob` na 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
```

O exemplo anterior criptografa a tabela restaurada usando uma chave AWS de propriedade. A parte dos metadados de restauração que especifica a criptografia usando a chave AWS-owned é:. `\"encryptionType\":\"Default\",\"kmsMasterKeyArn\":\"Not Applicable\"`

Para criptografar sua tabela restaurada usando uma chave AWS gerenciada, especifique os seguintes metadados de restauração:. `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"Not Applicable\"`

Para criptografar sua tabela restaurada usando uma chave gerenciada pelo cliente, especifique os seguintes metadados de restauração: `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"`*`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`*`\"`.

Restaurar um banco de dados do RDS

A restauração de um banco de dados do Amazon RDS exige a especificação de várias opções de restauração. Para obter mais informações sobre essas opções, consulte Backup e restauração de uma instância de banco de dados do Amazon RDS no Guia do usuário do Amazon RDS.

Use o AWS Backup console para restaurar os pontos de recuperação do Amazon RDS

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID do recurso do Amazon RDS que deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Para restaurar um recurso, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.

4. No painel Especificações de instância, aceite os valores predefinidos ou especifique as opções para as configurações de Mecanismo de banco de dados,Modelo de licença, Classe de instância de banco de dados,Multi AZ e Tipo de armazenamento. Por exemplo, se você quiser uma instância de banco de dados em espera, especifique Multi AZ.
5. No painel Configurações, especifique um nome exclusivo para todas as instâncias de banco de dados e clusters de sua propriedade Conta da AWS na região atual. O identificador de instância de banco de dados não diferencia letras maiúsculas de minúsculas, mas é armazenado com todas as letras minúsculas, como em "`mydbinstance`". Este é um campo obrigatório.
6. No painel Rede e Segurança, aceite os padrões ou especifique as opções para as configurações de Nuvem Privada Virtual (VPC), grupo de sub-rede, Acessibilidade pública (geralmente Sim) e zona de disponibilidade.
7. No painel Opções de banco de dados, aceite os valores predefinidos ou especifique as opções para as configurações de Porta de banco, de dados, Grupo de parâmetros de banco de dados, Grupo de opções, Copiar tags para snapshots, e Autenticação de banco de dados de IAM habilitada.
8. Em Criptografia, use as configurações padrão. Se a instância de banco de dados de origem do snapshot tiver sido criptografada, a instância de banco de dados restaurada também será criptografada. Não é possível remover essa criptografia.
9. No painel Exportações de registros, escolha os tipos de log a serem publicados no Amazon CloudWatch Logs. O Perfil do IAM já está definido.
10. No painel Manutenção, aceite o valor predefinido ou especifique a opção para Atualização de versão secundária automática.
11. No painel de Restaurar perfil, escolha o perfil do IAM que o AWS Backup assumirá para essa restauração.
12. Depois que todas as configurações tiverem sido especificadas, escolha Restaurar backup.

    O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.

Use a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do Amazon RDS

Usar `StartRestoreJob`. Para obter informações sobre os metadados e valores aceitos, consulte `RestoreDBInstanceFromDBSnapshot` na Referência da API do Amazon RDS. Além disso, AWS

Backup aceita os seguintes atributos somente informativos. No entanto, incluí-los não afetará a restauração:

```
EngineVersion
KmsKeyId
Encrypted
vpcId
```

Restaurar um cluster do Aurora

Use o AWS Backup console para restaurar os pontos de recuperação do Aurora

AWS Backup restaura seu cluster Aurora; ele não cria nem anexa uma instância do Amazon RDS ao seu cluster. Nas etapas a seguir, você criará e anexará uma instância do Amazon RDS ao seu cluster do Aurora restaurado usando a CLI.

A restauração de um cluster do Aurora exige a especificação de várias opções de restauração. Para obter informações sobre essas opções, consulte Visão geral de backup e restauração de um cluster de banco de dados do Aurora no Guia do usuário do Amazon Aurora. As especificações das opções de restauração podem ser encontradas no guia da API para `RestoreDBClusterFromSnapshot`.

Como restaurar um cluster de banco de dados do Amazon Aurora

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID de recurso do Aurora que você deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Para restaurar um recurso, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.
4. No painel Especificações de instância, aceite os padrões ou especifique as opções para as configurações de Mecanismo de banco de dados, Versão do mecanismo de banco de dados e Tipo de capacidade.

> **Note**
>
> Se o tipo de capacidade Sem servidor estiver selecionado, um painel de Configurações de capacidade será exibido. Especifique as opções para as configurações de Unidade

de capacidade mínima do Aurora e Unidade de capacidade máxima do Aurora ou escolha opções diferentes na seção Configuração de dimensionamento adicional.

5. No painel Configurações, especifique um nome exclusivo para todas as instâncias de cluster de banco de dados de sua propriedade Conta da AWS na região atual.
6. No painel Rede e segurança aceite os valores predefinidos ou especifique as opções para a configurações de Nuvem privada virtual (VPC), Grupo de sub-redes e Zona de disponibilidade.
7. No painel Opções de banco de dados, aceite os valores predefinidos ou especifique as opções para as configurações de Porta de banco, de dados, Grupo de parâmetros de clusters de banco de dados e Autenticação de banco de dados de IAM habilitada.
8. No painel Backup, aceite o valor predefinido ou especifique a opção para a configuração de Copiar tags para snapshots.
9. No painel Backtrack, aceite o valor predefinido ou especifique as opções para as configurações de Ativar backtrack ou Desativar backtrack.
10. No painel Criptografia, aceite os valores predefinidos ou especifique as opções para as configurações de Habilitar criptografia ou Desabilitar criptografia.
11. No painel Exportações de registros, escolha os tipos de log a serem publicados no Amazon CloudWatch Logs. O Perfil do IAM já está definido.
12. No painel de Restaurar perfil, escolha o perfil do IAM que o AWS Backup assumirá para essa restauração.
13. Depois de especificar todas as configurações, escolha Restore backup (Restaurar backup).

    O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.
14. Após a conclusão da restauração, conecte o cluster do Aurora restaurado a uma instância do Amazon RDS.

    Usando a AWS CLI:

    - Para Linux, macOS ou Unix:

      ```
      aws rds create-db-instance --db-instance-identifier sample-instance \
                    --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
      instance-class db.r4.large
      ```

    - 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 backups e point-in-time restauração contínuos (PITR) para obter informações sobre backups contínuos e restauração em um momento escolhido.

Use a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do Aurora

Usar `StartRestoreJob`. É possível especificar os seguintes metadados durante as restaurações do 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;
```

Exemplo:

```
"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\":\"[]\"}"
```

Restaurar uma instância do Amazon EC2

Quando você restaura uma instância do EC2, AWS Backup cria uma Amazon Machine Image (AMI), uma instância, o volume raiz do Amazon EBS, volumes de dados do Amazon EBS (se o recurso protegido tiver volumes de dados) e snapshots do Amazon EBS. Você pode personalizar algumas configurações da instância usando o AWS Backup console ou um número maior de configurações usando o AWS CLI ou um AWS SDK.

As seguintes considerações se aplicam à restauração de instâncias do EC2:

- AWS Backup configura a instância restaurada para usar o mesmo par de chaves que o recurso protegido usou originalmente. Você não pode especificar um par de chaves diferente para a instância restaurada durante o processo de restauração.
- AWS Backup não faz backup nem restaura os dados do usuário que são usados ao iniciar uma instância do Amazon EC2.
- Ao configurar a instância restaurada, você pode escolher entre usar o mesmo perfil de instância usado originalmente pelo recurso protegido ou iniciar sem um perfil de instância. Isso é para evitar a possibilidade de aumento de privilégios. Você pode atualizar o perfil da instância restaurada usando o console do Amazon EC2.

  Se você usar o perfil da instância original, deverá conceder AWS Backup as seguintes permissões, em que o ARN do recurso é o ARN da função do IAM associada ao perfil da instância.

  ```
  {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::account-id:role/role-name"
  },
  ```

- Durante uma restauração, todas as cotas e restrições de configuração do Amazon EC2 se aplicam.
- Se o cofre contendo seus pontos de recuperação do Amazon EC2 tiver uma trava de cofre, Considerações adicionais sobre segurança consulte para obter mais informações.

Use o AWS Backup console para restaurar os pontos de recuperação do Amazon EC2

você pode restaurar uma instância inteira do Amazon EC2 a partir de um único ponto de recuperação, incluindo o volume raiz, os volumes de dados e algumas definições de configuração da instância, como o tipo de instância e o par de chaves.

Para restaurar recursos do Amazon EC2 usando o console AWS Backup

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e, em seguida, escolha o ID do recurso Amazon EC2 para abrir a página de detalhes do recurso.
3. No painel Pontos de recuperação, escolha o botão de rádio ao lado da ID do ponto de recuperação a ser restaurado. No canto superior direito do painel, escolha Restaurar.
4. No painel Configurações de rede, usamos as configurações da instância protegida para selecionar os valores padrão para o tipo de instância, VPC, sub-rede, grupo de segurança e função do IAM da instância. Você pode usar esses valores padrão ou alterá-los conforme necessário.
5. No painel Restaurar função, use a função Padrão ou escolha uma função do IAM para especificar uma função do IAM que conceda AWS Backup permissão para restaurar o backup.
6. No painel Tags de recursos protegidos, selecionamos Copiar tags do recurso protegido para o recurso restaurado por padrão. Se você não quiser copiar essas tags, desmarque a caixa de seleção.
7. No painel Configurações avançadas, aceite os valores padrão para as configurações da instância ou altere-os conforme necessário. Para obter informações sobre essas configurações, escolha Informações para que a configuração abra seu painel de ajuda.
8. Ao terminar de configurar a instância, escolha Restaurar backup.

Restaure o Amazon EC2 com AWS CLI

Na interface da linha de comando, `start-restore-job`permite restaurar com até 32 parâmetros (incluindo alguns parâmetros que não são personalizáveis por meio do AWS Backup console).

A lista a seguir contém os metadados aceitos que podem ser passados para restaurar um ponto de recuperação do 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 aceita os seguintes atributos somente de informações. No entanto, incluí-los não afetará a restauração:

```
vpcId
```

Também é possível restaurar uma instância do Amazon EC2 sem incluir parâmetros armazenados. Essa opção está disponível na guia Recurso protegido no console do AWS Backup .

Restaurar um volume do Storage Gateway

Se você estiver restaurando um snapshot de AWS Storage Gateway volume, poderá optar por restaurar o snapshot como um volume do Storage Gateway ou como um volume do Amazon EBS. Isso ocorre porque AWS Backup se integra aos dois serviços, e qualquer snapshot do Storage Gateway pode ser restaurado em um volume do Storage Gateway ou em um volume do Amazon EBS.

Restaure o Storage Gateway por meio do AWS Backup console

Como restaurar um volume do Storage Gateway

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID de recurso do Storage Gateway que deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Para restaurar um recurso, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.
4. Especifique os parâmetros de restauração para o recurso. Os parâmetros de restauração inseridos são específicos do tipo de recurso selecionado.

   Em Tipo de recurso, escolha o AWS recurso a ser criado ao restaurar esse backup.
5. Se você escolher o volume do Storage Gateway, escolha um Gateway em um estado acessível. Escolha também o Nome do destino iSCSI.

   1. Para gateways de “Volume armazenado”, escolha um ID de disco.
   2. Em gateways de “Volume em cache”, escolha uma capacidade que seja, pelo menos, tão grande quanto a do recurso protegido.

   Se você escolher Volume do EBS, forneça os valores para o Tipo de volume, Tamanho (GiB) e escolha uma Zona de disponibilidade.
6. Para a função Restaurar, escolha a função do IAM que AWS Backup será assumida para essa restauração.

   > **Note**
   >
   > Se a função AWS Backup padrão não estiver presente na sua conta, uma função padrão será criada para você com as permissões corretas. Você poderá excluir essa função padrão ou torná-la inutilizável.
7. Escolha Restaurar backup.

   O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.

Restaure o Storage Gateway com AWS CLI

Na interface de linha de comandos, `start-restore-job` permite restaurar um volume do Storage Gateway.

A lista a seguir contém os metadados aceitos.

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and Região da AWS.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

Restaurar uma tabela do Amazon Timestream

Quando você restaura uma tabela do Amazon Timestream, há várias opções para configurar, incluindo o nome da nova tabela, o banco de dados de destino, suas preferências de alocação de armazenamento (armazenamento de memória e magnético) e qual função você usará para concluir o trabalho de restauração. Você também pode escolher um bucket do Amazon S3 no qual deseja armazenar os logs de erro. As gravações de armazenamento magnético são assíncronas, portanto, talvez você queira registrar os erros em log.

O armazenamento de dados do Timestream tem dois níveis: um armazenamento de memória e um armazenamento magnético. O armazenamento de memória é necessário, mas você tem a opção de transferir sua tabela restaurada para o armazenamento magnético após o término do tempo de memória especificado. O armazenamento de memória é otimizado para gravações de dados de alto rendimento e point-in-time consultas rápidas. O armazenamento magnético é otimizado para gravações de dados retardatários com menor throughput, armazenamento de dados de longo prazo e consultas analíticas rápidas.

Ao restaurar uma tabela Timestream, você determina por quanto tempo deseja que a tabela permaneça em cada nível de armazenamento. Usando o console ou a API, você pode definir o tempo de armazenamento para ambos. Observe que o armazenamento é linear e sequencial. O Timestream armazenará primeiro a tabela restaurada no armazenamento da memória e, depois, fará a transição automática para o armazenamento magnético quando o tempo de armazenamento da memória for atingido.

> **Note**
>
> O período de retenção do armazenamento magnético deve ser igual ou maior que o período de retenção original (mostrado no canto superior direito do console), ou os dados serão perdidos.

Exemplo: você define a alocação do armazenamento de memória para armazenar dados por uma semana e define a alocação do armazenamento magnético para armazenar os mesmos dados por um ano. Quando os dados no armazenamento de memória completarem uma semana, eles serão movidos automaticamente para o armazenamento magnético. Depois, serão retido no armazenamento magnético por um ano. Ao final desse período, serão excluídos do Timestream e do AWS Backup.

Para restaurar uma tabela do Amazon Timestream usando o console AWS Backup

Você pode restaurar tabelas de Timestream no AWS Backup console que foram criadas por. AWS Backup

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID de recurso do Amazon Timestream que deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Para restaurar um recurso, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.
4. Especifique suas novas configurações de tabela, incluindo:
    a. Novo nome da tabela, com 2 a 256 caracteres (letras, números, hífens, pontos e sublinhados).
    b. Banco de dados de destino, escolhido no menu suspenso.
5. Alocação de armazenamento: defina a quantidade de tempo em que a tabela restaurada residirá primeiro no armazenamento de memória e defina a quantidade de tempo em que a tabela restaurada residirá no armazenamento magnético. O armazenamento de memória pode ser configurado para horas, dias, semanas ou meses. O armazenamento magnético pode ser configurado para dias, semanas, meses ou anos.

6. (Opcional) Habilitar gravações de armazenamento magnético: você tem a opção de permitir gravações de armazenamento magnético. Com essa opção marcada, os dados retardatários, que são dados com um carimbo de data/hora fora do período de retenção do armazenamento de memória, serão gravados diretamente no armazenamento magnético.
7. (Opcional) Local dos logs de erro do Amazon S3: é possível especificar um local do S3 no qual seus logs de erro serão armazenados. Navegue pelos arquivos do S3 ou copie e cole o caminho do arquivo do S3.

> **Note**
>
> Se você optar por especificar um local de log de erros do S3, a função usada para essa restauração deverá ter permissão para gravar em um bucket do S3 ou deverá conter uma política com essa permissão.

8. Escolha o perfil do IAM a ser passado para realizar restaurações. Você pode usar o perfil padrão do IAM ou especificar um diferente.
9. Clique em Restaurar backup.

Seus trabalhos de restauração estarão visíveis em recursos protegidos. É possível ver o status atual do trabalho de restauração clicando no botão Atualizar ou em CTRL-R.

Como restaurar uma tabela do Amazon Timestream usando API, CLI ou SDK

Use `StartRestoreJob` para restaurar uma tabela do Timestream via API.

Para restaurar um Timestream usando o AWS CLI, use a operação `start-restore-job.` e especifique os seguintes metadados:

```
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
```

Veja um exemplo de modelo:

```
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
```

Também é possível usar DescribeRestoreJob para ajudar com informações de restauração.

No AWS CLI, use a operação `describe-restore-job` e use os seguintes metadados:

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
```

Veja um exemplo de modelo:

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

Restaurar um cluster do Amazon Redshift

Você pode restaurar instantâneos automáticos e manuais no AWS Backup console ou por meio da CLI.

Quando você restaura um cluster do Amazon Redshift, as configurações originais do cluster são inseridas no console por padrão. É possível especificar configurações diferentes para as configurações abaixo. Ao restaurar uma tabela, você deve especificar os bancos de dados de origem e de destino. Para obter mais informações sobre essas configurações, consulte Restaurar um cluster a partir de um snapshot no Guia de gerenciamento do Amazon Redshift.

- Tabela única ou cluster: você pode optar por restaurar um cluster inteiro ou uma única tabela. Se você optar por restaurar uma única tabela, o banco de dados de origem, o esquema de origem e o nome da tabela de origem serão necessários, bem como o cluster de destino, o esquema e o nome da nova tabela.
- Tipo de nó: cada cluster do Amazon Redshift consiste em um nó líder e, pelo menos, um nó de computação. Ao restaurar um cluster, é necessário especificar o tipo de nó que atende aos seus requisitos de CPU, RAM, capacidade de armazenamento e tipo de drive.
- Número de nós: ao restaurar um cluster, é necessário especificar o número de nós necessários.
- Resumo da configuração
- Permissões de cluster

Para restaurar um cluster ou tabela do Amazon Redshift usando o console AWS Backup

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Configurações e o ID de recurso do Amazon Redshift que deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Para restaurar um recurso, no painel Pontos de recuperação, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.
4. Opções de restauração
    a. Restaurar o cluster a partir do snapshot ou
    b. Restaurar uma única tabela em um snapshot para um novo cluster. Se escolher essas opções, você deverá configurar o seguinte:
        i. Ative ou desative nomes com distinção entre maiúsculas e minúsculas.
        ii. Insira os valores da tabela de origem, incluindo o banco de dados, o esquema e a tabela. As informações da tabela de origem podem ser encontradas no console do Amazon Redshift.
        iii. Insira os valores da tabela de destino, incluindo o banco de dados, o esquema e a tabela.
5. Especifique as novas configurações do cluster, incluindo:

a. Para restauração de clusters: escolha Identificador de cluster, Tipo de nó e número de nós.

b. Especifique a zona de disponibilidade e as janelas de manutenção.

c. É possível associar funções adicionais clicando em Associar perfis do IAM.

6. Opcional Configurações adicionais:

a. A opção Usar padrões está ativada por padrão.

b. Use os menus suspensos para selecionar as configurações de rede e segurança, grupos de segurança de VPC, grupo de sub-redes de cluster e zona de disponibilidade.

c. Ative ou desative o Roteamento aprimorado da VPC.

d. Determine se você deseja tornar seu endpoint do cluster publicamente acessível. Se estiver, as instâncias e os dispositivos fora da VPC poderão se conectar ao seu banco de dados por meio do endpoint do cluster. Se estiver ativado, insira o endereço IP elástico.

7. Opcional: configuração do banco de dados. Você pode optar por inserir

a. Porta do banco de dados (digitando-a no campo de texto)

b. Grupos de parâmetros

8. Manutenção: Você pode escolher o

a. Janela de manutenção

b. Rastreamento de manutenção, entre atual, final ou pré-visualização. Isso controla qual versão do cluster será aplicada durante uma janela de manutenção.

9. O snapshot automatizado está definido como padrão.

a. Período de retenção de snapshot automático. O período de retenção deve ser de 0 a 35 dias. Escolha 0 para não criar snapshots automatizados.

b. O período de retenção manual de snapshots é de 1 a 3.653 dias.

c. Há uma caixa de seleção opcional para a realocação do cluster. Se for marcada, essa opção permitirá realocar o cluster em outra zona de disponibilidade. Depois de habilitar a realocação, você poderá usar o endpoint da VPC.

10. Monitoramento: depois que um cluster é restaurado, você pode configurar o monitoramento por meio do Amazon Redshift CloudWatch ou Amazon Redshift.

11. Escolha o perfil do IAM a ser passado para realizar restaurações. É possível usar o perfil padrão do IAM ou especificar um diferente.

Seus trabalhos de restauração estarão visíveis em Trabalhos. É possível ver o status atual do trabalho de restauração clicando no botão Atualizar ou em CTRL-R.

Restaurar um cluster do Amazon Redshift usando a API, a CLI ou o SDK

Use `StartRestoreJob` para restaurar um cluster do Amazon Redshift.

Para restaurar um Amazon Redshift usando o AWS CLI, use o comando `start-restore-job` e especifique os seguintes metadados:

```
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 obter mais informações, consulte RestoreFromClusterSnapshot na Referência da API do Amazon Redshift e restore-from-cluster-snapshot no Guia da AWS CLI .

Veja um exemplo de modelo:

```
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 Região da AWS
-\-endpoint-url URL
```

Exemplo:

```
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 \
```

Também é possível usar DescribeRestoreJob para ajudar com informações de restauração.

No AWS CLI, use a operação `describe-restore-job` e use os seguintes metadados:

```
Region
```

Veja um exemplo de modelo:

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region Região da AWS
```

Exemplo:

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
```

```
-\-region us-west-2 \
```

Restaurar um banco de dados SAP HANA em uma instância do Amazon EC2

Os bancos de dados SAP HANA em instâncias do EC2 podem ser restaurados usando o AWS Backup console, usando a API ou usando. AWS CLI

Tópicos

- Restaure um SAP HANA no banco de dados de instâncias do Amazon EC2 usando o console AWS Backup
- StartRestoreJob API para SAP HANA no EC2
- CLI para SAP HANA no EC2
- Solução de problemas

Restaure um SAP HANA no banco de dados de instâncias do Amazon EC2 usando o console AWS Backup

Observe que os trabalhos de backup e restauração envolvendo o mesmo banco de dados não podem ocorrer simultaneamente. Quando um trabalho de restauração do banco de dados SAP HANA está ocorrendo, as tentativas de fazer backup do mesmo banco de dados provavelmente resultarão em um erro: “Não é possível fazer backup do banco de dados enquanto ele estiver parado”.

1. Acesse o AWS Backup console usando as credenciais dos pré-requisitos.
2. No menu suspenso Local de destino da restauração, escolha um banco de dados para substituir pelo ponto de recuperação que você está usando para restaurar (observe que a instância que hospeda o banco de dados de destino de restauração também deve ter as permissões dos pré-requisitos).

> **Important**
>
> As restaurações do banco de dados SAP HANA são destrutivas. A restauração de um banco de dados substituirá o banco de dados no local de restauração de destino especificado.

3. Conclua esta etapa somente se você estiver executando uma restauração de cópia do sistema. Caso contrário, prossiga para a etapa 4.

   Restaurações de cópia do sistema são trabalhos de restauração nos quais o banco de dados de destino da restauração é diferente do banco de dados de origem que gerou o ponto de recuperação. Para restaurações de cópias do sistema, observe o comando `aws ssm-sap put-resource-permission` fornecido para você no console. Esse comando deve ser copiado, colado e executado na máquina que preencheu os pré-requisitos. Ao executar o comando, use as credenciais da função no pré-requisito em que você configura as permissões necessárias para registrar aplicações.

   ```
   // 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. Depois de escolher o local de restauração, você poderá ver o ID do recurso, o nome da aplicação, o tipo de banco de dados e a instância do EC2 do banco de dados de destino.
5. Opcionalmente, você pode abrir as Configurações avançadas de restauração para alterar a opção de restauração do catálogo. A seleção padrão é restaurar o catálogo mais recente do AWS Backup.
6. Clique em Restaurar backup.
7. O local de destino será substituído durante a (“restauração destrutiva”), portanto, você deverá fornecer a confirmação de que permite isso na próxima caixa de diálogo pop-up.

   a. Para continuar, você deve entender que o banco de dados existente será substituído pelo banco de dados que você está restaurando.

   b. Depois que entender isso, você deverá reconhecer que os dados existentes serão substituídos. Para confirmar isso e continuar, digite substituir no campo de entrada de texto.
8. Clique em Restaurar backup.

Se procedimento tiver êxito, um banner azul será exibido na parte superior do console. Isso significa que o trabalho de restauração está em andamento. Você será redirecionado automaticamente para a página Trabalhos, onde o trabalho de restauração será exibido na lista de trabalhos de restauração. Esse trabalho mais recente terá um status de `Pending`. É possível pesquisar e clicar na ID do

trabalho de restauração para ver os detalhes de cada trabalho de restauração. É possível atualizar a lista de trabalhos de restauração clicando no botão Atualizar para ver as alterações no status do trabalho de restauração.

StartRestoreJob API para SAP HANA no EC2

Esta ação recupera o recurso salvo identificado por um Nome do recurso da Amazon (ARN).

Sintaxe da solicitação

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Parâmetros de solicitação de URI: a solicitação não usa nenhum parâmetro de URI.

Corpo da solicitação: a solicitação aceita os seguintes dados no formato JSON:

IdempotencyTokenUma sequência de caracteres escolhida pelo cliente que você pode usar para distinguir entre chamadas idênticas para. `StartRestoreJob` Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

Metadados

Um conjunto de pares de chave/valor de metadados. Contém informações, como o nome do recurso, necessárias para restaurar um ponto de recuperação. É possível obter metadados de configuração sobre um recurso no momento em que o backup foi feito por meio de uma chamada a `GetRecoveryPointRestoreMetadata`. No entanto, valores além dos fornecidos por

`GetRecoveryPointRestoreMetadata` podem ser necessários para restaurar um recurso. Por exemplo, talvez seja necessário fornecer um novo nome de recurso caso o original já exista.

É necessário incluir metadados específicos para restaurar um SAP HANA na instância do Amazon EC2. Veja os StartRestoreJob metadados dos itens específicos do SAP HANA.

Para recuperar os metadados relevantes, você pode usar a chamada `GetRecoveryPointRestoreMetadata`.

Exemplo de um ponto de recuperação de banco de dados SAP HANA padrão:

```
"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"
    }
```

Exemplo de um ponto de recuperação de banco de dados SAP HANA padrão:

```
"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 no EC2

O comando `start-restore-job` recupera o recurso salvo identificado por um Nome do recurso da Amazon (ARN). A CLI seguirá a diretriz de API acima.

Resumo:

```
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]
```

Opções

`--recovery-point-arn` (string) é uma string na forma de um Número de recurso da Amazon (ARN) que identifica um ponto de recuperação de forma exclusiva. Por exemplo

`arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`

`--metadata` (mapa): um conjunto de pares de chave/valor de metadados. Contém informações, como o nome do recurso, necessárias para restaurar um ponto de recuperação. É possível obter metadados de configuração sobre um recurso no momento em que o backup foi feito por meio de uma chamada a `GetRecoveryPointRestoreMetadata`. No entanto, valores além dos fornecidos por `GetRecoveryPointRestoreMetadata` podem ser necessários para restaurar um recurso. É necessário incluir metadados específicos para restaurar um SAP HANA na instância do Amazon EC2.

- `aws:backup:request-id`: isso é qualquer string UUID usada para idempotência. Isso não altera sua experiência de restauração de forma alguma.
- `aws:backup:TargetDatabaseArn`: especifique o banco de dados para o qual você deseja restaurar. Isso é o SAP HANA no ARN do banco de dados do Amazon EC2.
- `CatalogRestoreOption`: especifique de onde restaurar seu catálogo. Um de `NO_CATALOG`, `LATEST_CATALOG_FROM_AWS_BACKUP`, `CATALOG_FROM_LOCAL_PATH`
- `LocalCatalogPath`: se o valor dos CatalogRestoreOption metadados for`CATALOG_FROM_LOCAL_PATH`, especifique o caminho para o catálogo local na sua instância do EC2. Isso deve ser um caminho de arquivo válido na sua instância do EC2.
- `RecoveryType`: no momento, `FULL_DATA_BACKUP_RECOVERY`, `POINT_IN_TIME_RECOVERY`, e os tipos de recuperação `MOST_RECENT_TIME_RECOVERY` são compatíveis.

chave = (string); valor = (string). Sintaxe simplificada:

```
KeyName1=string,KeyName2=string
```

Sintaxe do JSON:

```
{"string": "string"
  ...}
```

`--idempotency-token` é uma string escolhida pelo usuário que pode ser usada para distinguir entre chamadas idênticas a `StartRestoreJob`. Tentar novamente uma solicitação bem-sucedida com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

`--resource-type` é uma string que inicia um trabalho para restaurar um ponto de recuperação para um dos seguintes recursos: `SAP HANA on Amazon EC2` para SAP HANA no Amazon EC2. Opcionalmente, os recursos do SAP HANA podem ser marcados usando o comando `aws ssm-sap tag-resource`

Saída: `RestoreJobId` é uma string que Identifica de forma exclusiva o trabalho que restaura um ponto de recuperação.

Solução de problemas

Se algum dos erros a seguir ocorrer ao tentar uma operação de backup, consulte a resolução associada.

- Erro: erro de log de backup contínuo

  Para manter os pontos de recuperação para backups contínuos, os logs são criados pelo SAP HANA para todas as alterações. Quando os registros não estão disponíveis, o status de cada um desses pontos de recuperação contínuos é `STOPPED`. O último ponto de recuperação viável que pode ser usado para restaurar é aquele com o status de `AVAILABLE`. Se os dados de log estiverem ausentes no período entre os pontos de recuperação com um status `STOPPED` e os pontos com `AVAILABLE`, não é possível garantir que esses horários tenham uma restauração com êxito. Se você inserir uma data e hora dentro desse intervalo, AWS Backup tentará fazer o backup, mas usará o horário restaurável disponível mais próximo. Esse erro será mostrado pela mensagem `“Encountered an issue with log backups. Please check SAP HANA for details."`

  Resolução: no console, o horário restaurável mais recente, com base nos logs, será exibido. Você pode inserir uma hora mais recente do que a hora exibida. No entanto, se os dados desse período não estiverem disponíveis nos registros, AWS Backup usará o tempo restaurável mais recente.

- Erro:

  Resolução: Crie um caso de suporte no console ou entre em contato AWS Support com os detalhes da restauração, como o ID do trabalho de restauração.

- Erro: `The provided role arn:aws:iam::`*`ACCOUNT_ID`*`:role/ServiceLinkedRole cannot be assumed by AWS Backup`

  Resolução: certifique-se de que a função assumida ao chamar a restauração tenha as permissões necessárias para criar funções vinculadas ao serviço.

- Erro: `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:...`

  Resolução: certifique-se de que a função assumida ao chamar as permissões de restauração descritas nos pré-requisitos seja inserida corretamente.

- Erro: `b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n`

  Resolução: certifique-se de que o agente Backint tenha sido instalado corretamente. Verifique todos os pré-requisitos, especialmente Instalar o AWS BackInt Agente e o SAP em seu servidor AWS Systems Manager de aplicativos SAP e, em seguida, tente instalar o Agente novamente. BackInt

- Erro: `IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED`

  Resolução: restaure o trabalho de restauração foi cancelado pelo fluxo de trabalho do serviço. Tente fazer o trabalho de restauração novamente.

- Erro: `RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"`

  Resolução: uma instabilidade transitória da rede está ocorrendo na instância. Tente fazer a restauração novamente. Se esse problema ocorrer de forma consistente, tente adicionar `ForceRetry: "true"` ao arquivo de configuração do agente em `/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml`.

Para qualquer outro problema relacionado ao agente AWS Backint, consulte Solucionar problemas do Backint AWS Agent para SAP HANA.

Restaurar um cluster do DocumentDB

Use o AWS Backup console para restaurar os pontos de recuperação do Amazon DocumentDB

A restauração de um cluster do Amazon DocumentDB exige a especificação de várias opções de restauração. Para obter informações sobre essas opções, consulte Restaurar a partir de um snapshot de cluster no Guia do desenvolvedor do Amazon DocumentDB.

Como restaurar um cluster do Amazon DocumentDB

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID de recurso do Amazon DocumentDB que deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Para restaurar um recurso, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.
4. No painel Configuração, aceite os padrões ou especifique as opções para o identificador do cluster, a versão do mecanismo, a classe da instância e o número de instâncias.

   - OBSERVAÇÃO: se a VPC padrão não existir durante a restauração, você deverá especificar uma sub-rede em outra VPC.
5. No painel Rede e Segurança, “Sem preferências” será exibido.
6. No ncryption-at-restpainel E, aceite o padrão ou especifique as opções para as configurações Ativar criptografia ou Desativar criptografia.
7. No painel Opções do cluster, digite a Porta e escolha o Grupo de parâmetros do cluster.
8. No painel Backup, escolha backup contínuo para point-in-time recuperação (PITR), backups de instantâneos agendados ou ambos.
9. No painel Exportações de registros, escolha os tipos de log a serem publicados no Amazon CloudWatch Logs. O Perfil do IAM já está definido.
10. No painel Manutenção, especifique uma janela de manutenção ou escolha Sem preferência.
11. No painel Tags, escolha Adicionar tag.
12. Em Proteção contra exclusão, escolha Habilitar a proteção contra exclusão.
13. Depois de especificar todas as configurações, escolha Restore backup (Restaurar backup).

    O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.
14. Após a conclusão da restauração, anexe o cluster do restaurado do Amazon DocumentDB a uma instância do Amazon RDS.

Use a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do Amazon DocumentDB

Primeiro, restaure o cluster. Usar `StartRestoreJob`. É possível especificar os seguintes metadados durante as restaurações do 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
```

Depois, anexe o cluster do Amazon DocumentDB restaurado a uma instância do Amazon RDS usando `create-db-instance`.

- Para Linux, macOS ou Unix:

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- 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
```

Restaurar um cluster do Neptune

Use o AWS Backup console para restaurar os pontos de recuperação do Amazon Neptune

A restauração de um banco de dados do Amazon Neptune exige a especificação de várias opções de restauração. Para obter informações sobre essas opções, consulte Restaurar a partir de um snapshot de cluster de banco de dados no Guia do desenvolvedor do Neptune.

Como restaurar um banco de dados Neptune

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos e o ID de recurso do Neptune que deseja restaurar.
3. Na página Detalhes do recurso é mostrada uma lista de pontos de recuperação para o ID de recurso selecionado. Para restaurar um recurso, no painel Backups, escolha o botão de opção ao lado do ID do ponto de recuperação do recurso. No canto superior direito do painel, escolha Restaurar.
4. No painel Especificações da instância, aceite os padrões ou especifique o mecanismo de banco de dados e a versão.
5. No painel Configurações, especifique um nome exclusivo para todas as instâncias de cluster de banco de dados de sua propriedade Conta da AWS na região atual. O identificador de clusters de banco de dados não diferencia letras maiúsculas de minúsculas, mas é armazenado com todas as letras minúsculas, como em "`mydbclusterinstance`". Este é um campo obrigatório.
6. No painel Opções de banco de dados, aceite os padrões ou especifique as opções para a Porta de banco, de dados e Grupo de parâmetros de clusters de banco de dados.
7. No painel Criptografia, aceite os valores predefinidos ou especifique as opções para as configurações de Habilitar criptografia ou Desabilitar criptografia.
8. No painel Exportações de registros, escolha os tipos de log a serem publicados no Amazon CloudWatch Logs. O Perfil do IAM já está definido.
9. No painel de Restaurar perfil, escolha o perfil do IAM que o AWS Backup assumirá para essa restauração.
10. Depois de especificar todas as configurações, escolha Restore backup (Restaurar backup).

    O painel Tarefas de restauração será exibido. Uma mensagem na parte superior da página fornece informações sobre o trabalho de restauração.

11. Após a conclusão da restauração, anexe o cluster restaurado do Neptune a uma instância do Amazon RDS.

Use a AWS Backup API, a CLI ou o SDK para restaurar os pontos de recuperação do Neptune

Primeiro, restaure o cluster. Usar `StartRestoreJob`. É possível especificar os seguintes metadados durante as restaurações do 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
```

Depois, anexe o cluster do Neptune restaurado a uma instância do Amazon RDS usando `create-db-instance`.

- Para Linux, macOS ou Unix:

```
aws neptune create-db-instance --db-instance-identifier sample-instance \
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

- 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 obter mais informações, consulte `RestoreDBClusterFromSnapshot` na Referência da API de gerenciamento do Neptune e o `restore-db-cluster-from-snapshot` no Guia da CLI do Neptune.

Restaurar CloudFormation backups da pilha

Um backup CloudFormation composto é uma combinação de um CloudFormation modelo e de todos os pontos de recuperação aninhados associados. Qualquer número de pontos de recuperação aninhados pode ser restaurado, mas o ponto de recuperação composto (que é o ponto de recuperação de nível superior) não pode ser restaurado.

Ao restaurar um ponto CloudFormation de recuperação de modelo, você cria uma nova pilha com um conjunto de alterações para representar o backup.

Restaure CloudFormation com o AWS Backup console;

No CloudFormation console, você pode ver o novo conjunto de pilhas e alterações. Para saber mais sobre conjuntos de alterações, consulte Atualizar pilhas usando conjuntos de alterações no Guia do usuário do AWS CloudFormation .

Determine de quais pontos de recuperação aninhados você deseja restaurar com sua CloudFormation pilha e, em seguida, restaure-os usando o AWS Backup console.

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Acesse Cofres de backup, selecione o cofre de backup que contém o ponto de recuperação desejado e clique em Pontos de recuperação.
3. Restaure o ponto de recuperação do AWS CloudFormation modelo.

    a. Clique no ponto de recuperação composto contendo os pontos de recuperação aninhados que você deseja restaurar para abrir a página Detalhes do ponto de recuperação composto.

    b. Em Pontos de recuperação aninhados, os pontos de recuperação aninhados serão exibidos. Cada ponto de recuperação terá um ID de ponto de recuperação, um status, um ID de recurso, um tipo de recurso, um tipo de backup e a hora em que o ponto de recuperação foi criado. Clique no botão de rádio ao lado do ponto de AWS CloudFormation recuperação e, em seguida, clique em Restaurar. Verifique se você está selecionando o

ponto de recuperação que tenha tipo de recurso: AWS CloudFormation e tipo de backup: backup.

4. Depois que o trabalho de restauração do CloudFormation modelo for concluído, seu AWS CloudFormation modelo restaurado ficará visível no AWS CloudFormation console em Pilhas.
5. Em Nomes de pilha, você deve encontrar o modelo restaurado com o status de `REVIEW_IN_PROGRESS`.
6. Clique no nome da pilha para ver seus detalhes.
7. Há guias abaixo do nome da pilha. Clique em Alterar conjuntos.
8. Execute o conjunto de alterações.
9. Após esses processos, os recursos na pilha original serão recriados na nova pilha. Os recursos com estado serão recriados vazios. Para recuperar os recursos com estado, volte para a lista de pontos de recuperação no AWS Backup console, selecione o ponto de recuperação necessário e inicie uma restauração.

Restaurar CloudFormation com AWS CLI

Na interface da linha de comando, `start-restore-job`permite restaurar uma CloudFormation pilha.

A lista a seguir contém os metadados aceitos para restaurar um 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
```

Testes de restauração

Tópicos

- Visão geral
- Comparação entre os testes de restauração e o processo de restauração

Visão geral

O teste de restauração, um recurso oferecido pela AWS Backup, fornece avaliação automatizada e periódica da viabilidade da restauração, bem como a capacidade de monitorar os tempos de duração do trabalho de restauração.

Primeiro, crie um plano de testes de restauração, fornecendo um nome para o plano, a frequência dos testes de restauração e o horário de início previsto. Depois, atribua os recursos que deseja incluir no plano. Em seguida, você escolhe incluir pontos de recuperação específicos ou aleatórios em seu teste. AWS Backup o backup infere de forma inteligente os metadados que serão necessários para que seu trabalho de restauração seja bem-sucedido.

Quando chegar o horário programado em seu plano, AWS Backup inicia os trabalhos de restauração com base em seu plano e monitora o tempo necessário para concluir a restauração.

Depois que o plano de teste de restauração for concluído, você poderá usar os resultados para mostrar a conformidade com os requisitos organizacionais ou de governança, como a conclusão bem-sucedida dos cenários de teste de restauração ou o tempo de conclusão do trabalho de restauração.

Opcionalmente, você pode usar Restaurar a validação do teste para confirmar os resultados do teste de restauração.

Quando a validação opcional for concluída ou a janela de validação for fechada, AWS Backup excluirá os recursos envolvidos no teste de restauração e os recursos serão excluídos de acordo com os SLAs de serviço.

Ao final do processo de teste, você poderá ver os resultados e o tempo de conclusão dos testes.

Comparação entre os testes de restauração e o processo de restauração

O recurso de testes de restauração executa trabalhos de restauração da mesma forma que as restaurações sob demanda e usa os mesmos pontos de recuperação (backups) de uma restauração sob demanda. Você verá chamadas para `StartRestoreJob` entrar CloudTrail (se tiver optado por participar) para cada trabalho iniciado pelo teste de restauração

No entanto, há algumas diferenças entre a operação de um teste de restauração programado e uma operação de restauração sob demanda:

	Testes de restauração	Restaurar
Conta	Uma prática recomendada é designar uma conta para ser usada nos testes de restauraç ão.	Você pode restaurar recursos de uma conta.
AWS Backup Audit Manager	É possível ativar um controle para confirmar se um teste de restauração atende aos objetivos de restauração especificados.	
Cadência	Periodicamente, como parte de um plano programado.	Sob demanda
Regionalidade	Disponível em todas as regiões comerciais em que AWS Backup opera, exceto Israel (Tel Aviv) Não disponível AWS GovCloud (Leste dos EUA),	Disponível em todas as regiões comerciais em que AWS Backup opera

	Testes de restauração	Restaurar
	AWS GovCloud (Oeste dos EUA), China (Pequim) e China (Ningxia).	
Recursos	Os tipos de recurso que você pode atribuir a um plano de testes incluem: Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, Amazon FSx (Lustre, ONTAP, OpenZFS, Windows), Amazon Neptune, Amazon RDS e Amazon S3.	Todos os recursos podem ser restaurados.
Resultados	Depois que o trabalho de teste de restauração for concluído , o recurso restaurado será excluído após o término da Restaurar a validação do teste janela.	Depois que o trabalho de restauração for concluído, a versão restaurada do recurso permanecerá.
Tags	Para tipos de recurso que oferecem suporte a etiquetas na restauração, os testes aplicam etiquetas na restauraç ão.	As etiquetas são opcionais para os recursos compatíveis.

Gerenciamento dos testes de restauração

Você pode criar, visualizar, atualizar ou excluir um plano de testes de restauração no console do AWS Backup.

Você pode usar a AWS CLI para realizar operações de forma programática para restaurar planos de testes. Cada CLI é específica para o AWS serviço em que se origina. Os comandos devem ser prefixados com `aws backup`.

Exclusão de dados

Quando um teste de restauração é concluído, AWS Backup começa a excluir os recursos envolvidos no teste. Essa exclusão não é instantânea. Cada recurso tem uma configuração subjacente que determina como esses recursos são armazenados e ciclos de vida. Por exemplo, se os buckets do Amazon S3 fizerem parte do teste de restauração, serão adicionadas regras de ciclo de vida ao bucket. Pode levar vários dias para que as regras sejam executadas e para que o bucket e seus objetos sejam totalmente excluídos, mas as cobranças só ocorrerão para esses recursos até o dia em que a regra de ciclo de vida for iniciada (por padrão, isso é 1 dia). A velocidade de exclusão dependerá do tipo de recurso.

Os recursos que fazem parte de um plano de testes de restauração contêm uma etiqueta chamada `awsbackup-restore-test`. Se um usuário remover essa tag, AWS Backup não poderá excluir o recurso no final do período de teste. Em vez disso, o usuário precisará excluí-la manualmente.

Para verificar por que os recursos podem não ter sido excluídos conforme o esperado, você pode pesquisar os trabalhos com falha no console ou usar a interface de linha de comandos para chamar a solicitação de API `DescribeRestoreJob` a fim de recuperar as mensagens de status de exclusão.

Os planos de backup (planos de teste sem restauração) ignoram os recursos criados pelo teste de restauração (aqueles com tag `awsbackup-restore-test` ou nome começando com`awsbackup-restore-test`).

Controle de custos

O recurso de testes de restauração tem um custo por teste de restauração. Dependendo dos recursos incluídos no plano de testes de restauração, os trabalhos de restauração que fazem parte do plano também poderão ter um custo. Para obter detalhes, consulte Definição de preço do AWS Backup.

Ao configurar um plano de testes de restauração pela primeira vez, você pode achar vantajoso incluir um número mínimo de tipos de recurso e recursos protegidos para se familiarizar com a funcionalidade, o processo e os custos médios envolvidos. Você pode atualizar um plano após sua criação para adicionar mais tipos de recurso e recursos protegidos.

Criar um plano de testes de restauração

Um plano de testes de restauração tem duas partes: criação do plano e atribuição de recursos.

Quando você usa o console, essas partes são sequenciais. Na primeira parte, defina o nome, a frequência e os horários de início. Durante a segunda parte, atribua recursos ao plano de testes.

Ao usar AWS CLI uma API, use primeiro `create-restore-testing-plan`. Depois de receber uma resposta bem-sucedida e o plano ter sido criado, use `create-restore-testing-selection` para cada tipo de recurso que você deseja incluir no plano.

Console

Parte I: Criar um plano de testes de restauração usando o console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Na navegação à esquerda, localize e selecione Teste de restauração.
3. Escolha Criar um plano de teste de restauração.
4. Geral
   a. Nome: digite um nome para o novo plano de testes de restauração. O nome não poderá ser alterado após a criação. Ele só pode conter caracteres alfanuméricos e sublinhados.
   b. Frequência de teste: escolha a frequência com que os testes de restauração serão executados.
   c. Horário inicial: defina o horário (em horas e minutos) em que você prefere que o teste comece. Você também pode definir o fuso horário local no qual deseja que o plano de testes de restauração opere.
   d. Comece em: Esse valor (em horas) é o período em que o teste de restauração está designado para começar. AWS Backup faz o possível para iniciar todos os trabalhos de restauração designados durante o início dentro do prazo e randomiza os horários de início dentro desse período.
5. Seleção do ponto de recuperação: aqui você define os cofres de origem, o intervalo de pontos de recuperação e os critérios de seleção para quais pontos de recuperação (backups) você deseja que façam parte do plano.
   a. Cofres de origem: escolha se deseja incluir todos os cofres disponíveis ou apenas cofres específicos para ajudar a filtrar quais pontos de recuperação podem estar no plano. Se você escolher a opção Cofres específicos, selecione no menu suspenso os cofres que deseja incluir.

b. Pontos de recuperação qualificados: especifique o período do qual os pontos de recuperação serão selecionados. Você pode selecionar de 1 a 365 dias, de 1 a 52 semanas, de 1 a 12 meses ou 1 ano.

c. Critérios de seleção: depois de especificar o intervalo de datas para os pontos de recuperação, você poderá escolher se deseja incluir o mais recente ou um aleatoriamente no plano. Talvez você queira escolher um aleatório para avaliar a integridade geral dos pontos de recuperação com mais frequência, caso a restauração de uma versão mais antiga seja necessária.

d. Pontos de oint-in-time recuperação P: Se seu plano incluir recursos com pontos de backup contínuo (point-in-time-restore/PITR), você poderá marcar essa caixa para que seu plano de teste inclua backups contínuos como pontos de recuperação elegíveis (consulte Disponibilidade de recursos por recurso para os quais tipos de recursos têm esse recurso).

6. (Opcional) Tags adicionadas ao plano de teste de restauração: você pode optar por adicionar até 50 etiquetas a um plano de testes de restauração. Cada etiqueta deve ser adicionada separadamente. Para adicionar uma etiqueta, selecione Adicionar nova tag.

Parte II: Atribuir recursos ao plano usando o console

Nesta seção, escolha os recursos dos quais fez backup para incluir no plano de testes de restauração. Você escolherá o nome da atribuição de recursos, escolherá o perfil que usará para o teste de restauração e definirá o período de retenção antes da limpeza. Depois, você selecionará o tipo de recurso, selecionará o escopo e, opcionalmente, refinará sua seleção com etiquetas.

> **Tip**
>
> Para voltar ao plano de testes de restauração ao qual você deseja adicionar recursos, acesse o console do AWS Backup, selecione Teste de restauração, encontre seu plano de testes preferido e escolha-o.

1. Geral

a. Nome da atribuição de recursos: insira um nome para essa atribuição de recursos usando uma string de caracteres alfanuméricos e sublinhados, sem nenhum espaço em branco.

b. Perfil do IAM para restauração: o teste deve usar um perfil do Identity and Access Management (IAM) designado por você. Você pode escolher a função AWS Backup padrão ou outra. Se o AWS Backup padrão ainda não existir quando você concluir esse processo, ele AWS Backup será criado automaticamente com as permissões necessárias. O perfil do IAM escolhido para os testes de restauração deve conter as permissões encontradas em AWSBackupServicePolicyForRestores.

c. Período de retenção antes da limpeza: durante um teste de restauração, os dados de backup são restaurados temporariamente. Por padrão, esses dados são excluídos após a conclusão do teste. Você tem a opção de atrasar a exclusão desses dados caso queira executar a validação da restauração.

   Se você planeja executar a validação, selecione a opção Reter por um número específico de horas e insira um valor de 1 a 168 horas (ambos incluídos). Observe que a validação pode ser executada de forma programática, mas não pelo console do AWS Backup .

2. Recursos protegidos:

   a. Selecione o tipo de recurso: selecione quais tipos de recurso e o escopo de quais backups desses tipos deseja incluir no plano de testes de recursos. Cada plano pode conter vários tipos de recurso, mas cada tipo de recurso deve ser atribuído ao plano individualmente.

   b. Escopo da seleção de recursos: depois de escolher o tipo, selecione se você deseja incluir todos os recursos protegidos disponíveis desse tipo ou se deseja incluir somente recursos protegidos específicos.

   c. (Opcional) Refine a seleção de recursos usando tags: se os backups tiverem etiquetas, você poderá usá-las para filtrar a fim de selecionar recursos protegidos específicos. Insira a chave de etiqueta, a condição para que essa chave seja ou não incluída e o valor da chave. Depois, selecione o botão Adicionar etiquetas.

      As etiquetas nos recursos protegidos são avaliadas verificando as etiquetas no ponto de recuperação mais recente no cofre de backup que contém o recurso protegido.

3. Parâmetros de restauração: determinados recursos exigem a especificação de parâmetros na preparação para um trabalho de restauração. Na maioria dos casos, AWS Backup inferirá os valores com base no backup armazenado.

   Em geral, é recomendável manter esses parâmetros, mas você pode alterar os valores escolhendo uma seleção diferente no menu suspenso. Exemplos em que a alteração dos

valores pode ser ideal incluem a substituição de chaves de criptografia, configurações do Amazon FSx em que os dados não podem ser inferidos e a criação de sub-redes.

Por exemplo, se um banco de dados do RDS for um dos tipos de recurso que você atribui ao plano de testes de restauração, parâmetros que incluem zona de disponibilidade, nome do banco de dados, classe da instância de banco de dados e grupo de segurança da VPC aparecerão com valores inferidos que você poderá alterar, se aplicável.

AWS CLI

O comando `CreateRestoreTestingPlan` da CLI é usado para criar um plano de testes de restauração.

O plano de testes deve conter:

- `RestoreTestingPlan`, que deve conter um único `RestoreTestingPlanName`
- Expressão cron `ScheduleExpression`
- `RecoveryPointSelection`

  Embora tenha um nome semelhante, NÃO é o mesmo que`RestoreTestingSelection`.

  `RecoveryPointSelection`tem cinco parâmetros (três obrigatórios e dois opcionais). Os valores especificados determinam qual ponto de recuperação está incluído no teste de restauração. Você deve indicar com `Algorithm` se deseja o ponto de recuperação mais recente dentro do seu `SelectionWindowDays` ou se deseja um ponto de recuperação aleatório e deve indicar por meio `IncludeVaults` de quais cofres os pontos de recuperação podem ser escolhidos.

Uma seleção pode ter um ou mais ARNs de recursos protegidos ou ter uma ou mais condições, mas não pode ter ambos.

Você também pode incluir:

- `ScheduleExpressionTimezone`
- `Tags`
- `CreatorRequestId`
- `StartWindowHours`

Use o comando `create-restore-testing-plan` da CLI.

Depois que o plano for criado com sucesso, você precisará atribuir recursos a ele usando `create-restore-testing-selection`.

Isso consiste em `RestoreTestingSelectionName`, `ProtectedResourceType` e um dos seguintes:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Cada tipo de recurso protegido pode ter um único valor. Uma seleção de testes de restauração pode incluir um valor curinga (“*”) para `ProtectedResourceArns` com `ProtectedResourceConditions`. Como alternativa, você pode incluir até 30 ARNs de recursos protegidos específicos em `ProtectedResourceArns`.

Determinação do ponto de recuperação

Cada vez que um plano de teste é executado (de acordo com a frequência e o horário de início especificados), um ponto de recuperação qualificado por recurso protegido selecionado é restaurado pelo teste de restauração. Se nenhum ponto de recuperação de um recurso atender aos critérios de seleção do ponto de recuperação, esse recurso não será incluído no teste.

Um ponto de recuperação para um recurso protegido em uma seleção de teste é elegível se atender aos critérios do período de tempo especificado e incluir cofres no plano de teste de restauração.

Um recurso protegido será selecionado se a seleção de teste do recurso incluir o tipo de recurso e se uma das seguintes condições for verdadeira:

- O ARN do recurso é especificado nessa seleção; ou,
- As condições da tag nessa seleção correspondem às tags no ponto de recuperação mais recente do recurso.

Atualizar um plano de testes de restauração

Você pode atualizar partes de um plano de testes de restauração e as seleções de recursos nele contidas pelo console ou pela AWS CLI.

Console

Atualizar planos e seleções de testes de restauração no console

Ao visualizar a página de detalhes do plano de testes de restauração no console, você pode editar (atualizar) muitas das configurações do plano. Para fazer isso:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Na navegação à esquerda, localize e selecione Teste de restauração.
3. Selecione o botão Edit.
4. Ajuste a frequência, o horário de início e o tempo que o teste terá para começar após o horário de início escolhido.
5. Salve as alterações.

AWS CLI

Atualize os planos e as seleções de testes de restauração por meio de AWS CLI

Solicita UpdateRestoreTestingPlane UpdateRestoreTestingSelectionpode ser usado para enviar atualizações parciais para um plano ou seleção específica. Os nomes não podem ser alterados, mas você pode atualizar outros parâmetros. Inclua somente os parâmetros que você deseja alterar em cada solicitação.

Antes de enviar uma solicitação de atualização, use GetRestoreTestingPlane GetRestoreTestingSelectionpara determinar se a sua RestoreTestingSelection contém ARNs específicos ou se usa o caractere curinga e as condições.

Se a seleção de testes de restauração tiver ARNs especificados (em vez de curinga) e você quiser alterá-la para um caractere curinga com condições, a solicitação de atualização deverá incluir o caractere curinga de ARN e as condições. Uma seleção pode ter ARNs de recursos protegidos ou usar o caractere curinga com condições, mas não pode ter ambos.

- `get-restore-testing-plan`
- `get-restore-testing-selection`
- `update-restore-testing-plan`
- `update-restore-testing-selection`

Visualizar os planos de testes de restauração existentes

Console

Visualizar detalhes sobre um plano de testes de restauração existente e os recursos atribuídos no console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Na navegação à esquerda, selecione Teste de restauração. A tela mostra os planos de testes de restauração. Por padrão, os planos são exibidos em ordem de última execução.
3. Selecione o link de um plano para ver os detalhes, incluindo um resumo do plano, o nome, a frequência, o horário de início e o tempo para início.

Você também pode visualizar os recursos protegidos nesse plano, os trabalhos de testes de restauração dos últimos 30 dias incluídos nesse plano e todas as etiquetas que você possa ter criado para fazer parte desse plano de testes.

AWS CLI

Obter detalhes sobre um plano de testes de restauração existente e uma seleção de testes usando a linha de comando

- `list-restore-testing-plan`
- `list-restore-testing-selections`
- `get-restore-testing-plan`
- `get-restore-testing-selection`

Visualizar trabalhos de testes de restauração

Console

Veja os trabalhos de testes de restauração existentes no console

Os trabalhos de testes de restauração estão incluídos na página de trabalhos de restauração.

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.

2. Navegue até a página Trabalhos.

   Você também pode selecionar Teste de restauração, depois escolher um plano de testes de restauração para ver os detalhes e os trabalhos associados a ele.

3. Selecione a guia Tarefas de restauração.

   Nessa página, você pode ver o status, o tempo de restauração, o tipo de restauração, o ID do recurso, o tipo de recurso, o plano de testes de restauração ao qual o trabalho pertence, o horário de criação e o ID do ponto de recuperação do trabalho de restauração.

   Os trabalhos incluídos em um plano de testes de restauração têm o tipo de restauração Teste.

Os trabalhos de testes de restauração têm várias categorias de status:

- Um tipo de Status que requer atenção fica sublinhado. Passe o mouse sobre o status para ver detalhes adicionais, caso estejam disponíveis.
- Um status de validação será exibido se Restaurar a validação do teste tiver sido iniciado no teste (não disponível no console).
- O status da exclusão indica o status dos dados gerados por um teste de restauração. Há três status de exclusão possíveis: Bem-sucedida, Excluindo e Com falha.

  Se a exclusão de um trabalho de testes de restauração falhar, você precisará remover o recurso manualmente, pois o fluxo de testes de restauração não pôde concluí-lo automaticamente. Muitas vezes, uma falha na exclusão será acionada se a etiqueta `awsbackup-restore-test` for removida do recurso.

AWS CLI

Visualizar os trabalhos de testes de restauração existentes pela linha de comandos

- `list-restore-jobs-by-protected-resource`

Excluir um plano de testes de restauração

Console

Excluir plano de testes de restauração no console

1. Acesse Visualizar os planos de testes de restauração existentes para ver seus planos de testes de restauração atuais.
2. Na página de detalhes do plano de testes de restauração, exclua um plano selecionando Excluir.
3. Depois de selecionar a opção para excluir, uma tela pop-up de confirmação aparecerá para confirmar que você deseja excluir o plano. Nessa tela, o nome do plano de testes de restauração específico será exibido em negrito. Para continuar, digite o nome exato do plano de testes com distinção entre maiúsculas e minúsculas, incluindo sublinhados, traços e pontos.

   Se a opção Excluir plano de teste de restauração não puder ser selecionada, insira novamente o nome até que ele corresponda ao nome exibido. Quando estabelecer correspondência exata, a opção de excluir o plano de testes de restauração poderá ser selecionada.

AWS CLI

Excluir plano de testes de restauração pela linha de comandos

O comando CLI DeleteRestoreTestingSelectionpode ser usado para excluir uma seleção de teste de restauração. Inclua `RestoreTestingPlanName` e `RestoreTestingSelectionName` na solicitação.

Todas as seleções de testes associadas a um plano de testes devem ser excluídas antes de excluir o plano de testes. Depois que todas as seleções de teste forem excluídas, você poderá usar a solicitação da API DeleteRestoreTestingPlanpara excluir um plano de teste de restauração. Você precisa incluir `RestoreTestingPlanName`.

- `delete-restore-testing-selection`
- `delete-restore-testing-plan`

Auditar testes de restauração

Restaure as integrações de teste com o AWS Backup Audit Manager para ajudá-lo a avaliar se um recurso restaurado foi concluído dentro do tempo de restauração desejado.

Para obter mais informações, consulte o controle Tempo de restauração para recursos cumpre a meta em AWS Backup Audit Manager controls and remediation.

Cotas e parâmetros de testes de restauração

- 100 planos de testes de restauração
- 50 etiquetas podem ser adicionadas a cada plano de testes de restauração
- 30 seleções por plano
- 30 ARNs de recursos protegidos por seleção
- 30 condições de recursos protegidos por seleção (incluindo aquelas dentro de `StringEquals` e `StringNotEquals`)
- 30 seletores de cofre por seleção
- Máximo de dias da janela de seleção: 365 dias
- Horas da janela de início: mín. de 1 hora, máx. de 168 horas (7 dias)
- Comprimento máximo do nome do plano: 50 caracteres
- Comprimento máximo do nome da seleção: 50 caracteres

Informações adicionais sobre os limites podem ser conferidas em AWS Backup cotas.

Solução de problemas de falha de teste de restauração

Se você tiver trabalhos de teste de restauração com um status de restauração de`Failed`, os motivos a seguir podem ajudá-lo a determinar a causa e a solução.

As mensagens de erro podem ser visualizadas no AWS Backup console na página de detalhes do status do trabalho ou usando os comandos `list-restore-jobs-by-protected-resource` da CLI ou. `list-restore-jobs`

1. Erro:

   Solução 1: atualize sua seleção de teste de restauração e substitua o parâmetro`SubnetId`. O AWS Backup console exibe esse parâmetro como “Sub-rede”.

Solução 2: recrie a VPC padrão.

Tipos de recursos afetados: Amazon EC2

2. Erro:

   Solução 1: atualize sua seleção de teste de restauração e substitua o parâmetro de `SubnetId` restauração. O AWS Backup console exibe esse parâmetro como “Sub-rede”.

   Solução 2: crie uma sub-rede padrão na VPC padrão.

   Tipos de recursos afetados: Amazon EC2

3. Erro:

   Solução 1: atualize sua seleção de teste de restauração e substitua o parâmetro de `DBSubnetGroupName` restauração. O AWS Backup console exibe esse parâmetro como Grupo de sub-rede.

   Solução 2: crie uma sub-rede padrão na VPC padrão.

   Tipos de recursos afetados: Amazon Aurora, Amazon DocumentDB, Amazon RDS, Neptune

4. Erro:*`IAM Role cannot be assumed by AWS Backup`*.

   Solução: A função de restauração deve ser assumida por. AWS Backup Atualize a política de confiança da função no IAM para permitir que ela seja assumida `"backup.amazonaws.com"` ou atualize sua seleção de testes de restauração para usar uma função que seja assumida por. AWS Backup

   Tipos de recursos afetados: todos

5. Erro: *`Access denied to KMS key.`* ou *`The specified AWS KMS key`* `ARN` *`does not exist, is not enabled or you do not have permissions to access it.`*

   Solução: verifique o seguinte:

   a. A função de restauração tem acesso à AWS KMS chave usada para criptografar seus backups e, se aplicável, à chave KMS usada para criptografar o recurso restaurado.

b. As políticas de recursos nas chaves KMS acima permitem que a função de restauração as acesse.

Se as condições acima ainda não forem atendidas, configure a função de restauração e as políticas de recursos para acesso adequado. Em seguida, execute o trabalho de teste de restauração novamente.

Tipos de recursos afetados: todos

6. Erros: *User ARN is not authorized to perform action on resource because no identity based policy allows the action.* ou *Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx*.

   Solução: a função de restauração não tem permissões adequadas. Atualize as permissões no IAM para a função de restauração.

   Tipos de recursos afetados: todos

7. Erros: *User ARN is not authorized to perform action on resource because no resource-based policy allows the action.* ou *User ARN is not authorized to perform action on resource with an explicit deny in a resource based policy.*

   Solução: a função de restauração não tem acesso adequado ao recurso especificado na mensagem. Atualize a política de recursos no recurso mencionado.

   Tipos de recursos afetados: todos

Metadados inferidos de testes de restauração

A restauração de um ponto de recuperação requer metadados de restauração. Para realizar testes de restauração, o AWS Backup infere automaticamente os metadados que provavelmente resultarão em uma restauração bem-sucedida. O comando `get-restore-testing-inferred-metadata` pode ser usado para visualizar o que AWS Backup será inferido. O comando `get-restore-job-metadata` retorna o conjunto de metadados inferidos por. AWS Backup Observe que, para alguns tipos de recursos (Amazon FSx), não AWS Backup é possível inferir um conjunto completo de metadados.

Os metadados de restauração inferidos são determinados durante o processo de testes de restauração. Você pode substituir determinadas chaves de metadados de restauração incluindo o parâmetro `RestoreMetadataOverrides` no corpo de `RestoreTestingSelection`. Algumas substituições de metadados não estão disponíveis no console. AWS Backup

Cada recurso compatível tem chaves e valores de metadados de restauração inferidos e chaves de metadados de restauração substituíveis. Somente pares de chave e valor de `RestoreMetadataOverrides` ou pares de chave e valor aninhados marcados com *`obrigatório para restauração bem-sucedida`* devem ser incluídos; os demais são opcionais. Observe que valores de chave não diferenciam entre maiúsculas e minúsculas.

> **Important**
>
> AWS Backup pode inferir que um recurso deve ser restaurado para a configuração padrão, como uma instância do Amazon EC2 ou um cluster do Amazon RDS restaurado para a VPC padrão. No entanto, se o padrão não estiver presente, por exemplo, a VPC ou sub-rede padrão tiver sido excluída e nenhuma substituição de metadados tiver sido inserida, a restauração não será bem-sucedida.

Tipo de recurso	Chaves e valores de metadados de restauração inferidos	Metadados substituíveis

DynamoDB	`deletionProtection` , em que o valor é definido como `false`
	
	`encryptionType` é definido como `Default`
	
	`targetTableName` , em que o valor é definido como um valor aleatório que começa com `awsbackup-restore-test-`
		`encryptionType`
		
		`kmsMasterKeyArn`

Tipo de recurso	Chaves e valores de metadados de restauração inferidos	Metadados substituíveis

Amazon EBS	`availabilityZone` , cujo valor é definido como uma zona de disponibilidade aleatória
	
	`encrypted` , cujo valor é definido como `true`
		`availabilityZone`
		
		`kmsKeyId`

Amazon EC2	O valor de `disableApiTermination` é definido como `false`
	
	O valor de `instanceType` é definido como o instanceType do ponto de recuperação que está sendo restaurado
	
	O valor de `requiredImdsV2` é definido como `true`
		`iamInstanceProfileName` o valor pode ser nulo ou `UseBackedUpValue`
		
		`instanceType`
		
		`requireImdsV2`
		
		`securityGroupIds`
		
		`subnetId`

Tipo de recurso	Chaves e valores de metadados de restauração inferidos	Metadados substituíveis
Amazon EFS	O valor de `encrypted` é definido como `true` O valor de `file-system-id` é definido como o ID do sistema de arquivos do ponto de recuperação que está sendo restaurado `kmsKeyId value` é definido como `alias/aws/elasticfilesystem` O valor de `newFileSystem` é definido como `true` O valor de `performanceMode` é definido como `generalPurpose`	`kmsKeyId`

Amazon FSx para Lustre	`lustreConfiguration` tem chaves aninhadas. Uma chave aninhada é `automaticBackupRetentionDays`, cujo valor é definido como `0`	`kmsKeyId`
		
		`lustreConfiguration` tem a chave aninhada `logConfiguration`
		
		`securityGroupIds`
		
		`subnetIds`, *obrigatório para restauração bem-sucedida*

Tipo de recurso	Chaves e valores de metadados de restauração inferidos	Metadados substituíveis
Amazon FSx para ONTAP NetApp	`name` é definido como um valor aleatório que começa com `awsbackup_restore_test_` `ontapConfiguration` tem chaves aninhadas, incluindo: • `junctionPath` , em que `/name` é o nome do volume que está sendo restaurado • `sizeInMegabytes` , cujo valor é definido como o tamanho, em megabytes, do ponto de recuperação que está sendo restaurado • `snapshotPolicy` , em que o valor é definido como `none`	`ontapConfiguration` tem chaves aninhadas substituíveis específicas, incluindo: • `junctionPath` • `ontapVolumeType` • `securityStyle` • `sizeInMegabytes` • `storageEfficiencyEnabled` • `storageVirtualMachineId` , *obrigatório para restauração bem-sucedida* • `tieringPolicy`

Tipo de recurso	Chaves e valores de metadados de restauração inferidos	Metadados substituíveis

Amazon FSx para OpenZFS	`openZfzConfiguration` , que tem chaves aninhadas, incluindo:
	• `automaticBackupRetentionDays` com valor definido como `0`
	• `deploymentType` com valor definido como o tipo de implantação do ponto de recuperação que está sendo restaurado
	• `throughputCapacity` , cujo valor é baseado em `deploymentType` . Se `deploymentType` for `SINGLE_AZ_1` , o valor será definido como 64; se `deploymentType` for `SINGLE_AZ_2` or `MULTI_AZ_1` , o valor será definido como `160`
		`kmsKeyId`
		`openZfsConfiguration` tem chaves aninhadas substituíveis específicas, incluindo:
		• `deploymentType`
		• `throughputCapacity`
		• `diskiopsConfiguration`
		`securityGroupIds`
		`subnetIds`

Tipo de recurso	Chaves e valores de metadados de restauração inferidos	Metadados substituíveis

Amazon FSx para Windows File Server	`windowsConfiguration` , que tem chaves aninhadas, incluindo:
	• `automaticBackupRetentionDays` com valor definido como `0`
	• `deploymentType` com valor definido como o tipo de implantação do ponto de recuperação que está sendo restaurado
	• `throughputCapacity` com valor definido como 8
		`kmsKeyId`
		`securityGroupIds`
		`subnetIds` , *obrigatório para restauração bem-sucedida*
		`windowsConfiguration` , com chaves aninhadas substituíveis específicas
		• `throughputCapacity`
		• `activeDirectoryId` *necessário para uma restauração bem-sucedida, se não `selfManagedActiveDirectoryConfiguration` estiver incluído*
		• `selfManagedActiveDirectoryConfiguration` *necessário para uma restauração bem-sucedida, se não `activeDirectoryId` estiver incluído*
		• `preferredSubnetId`

Tipo de recurso	Chaves e valores de metadados de restauração inferidos	Metadados substituíveis

Clusters do Amazon RDS, Aurora, Amazon DocumentDB e Amazon Neptune	`availabilityZones` com valor definido como uma lista de até três zonas de disponibilidade aleatórias
	
	`dbClusterIdentifier` com um valor aleatório que começa com `awsbackup-restore-test`
	
	`engine` com valor definido como o mecanismo do ponto de recuperação que está sendo restaurado
		`availabilityZones`
		
		`databaseName`
		
		`dbClusterParameterGroupName`
		
		`dbSubnetGroupName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`engine`
		
		`engineMode`
		
		`engineVersion`
		
		`kmskeyId`
		
		`port`
		
		`optionGroupName`
		
		`scalingConfiguration`
		
		`vpcSecurityGroupIds`

Tipo de recurso	Chaves e valores de metadados de restauração inferidos	Metadados substituíveis

Instâncias do Amazon RDS	`dbInstanceIdentifier` com um valor aleatório que começa com `awsbackup-restore-test-`
	
	`deletionProtection` com valor definido como `false`
	
	`multiAz` com valor definido como `false`
	
	`publiclyAccessible` com valor definido como falso
		`allocatedStorage`
		
		`availabilityZones`
		
		`dbInstanceClass`
		
		`dbName`
		
		`dbParameterGroupName`
		
		`dbSubnetGroupName`
		
		`domain`
		
		`domainIamRoleName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`iops`
		
		`licensemodel`
		
		`multiAz`
		
		`optionGroupName`
		
		`port`
		
		`processorFeatures`
		
		`publiclyAccessible`
		
		`storageType`

Tipo de recurso	Chaves e valores de metadados de restauração inferidos	Metadados substituíveis
		`vpcSecurityGroupIds`

Amazon Simple Storage Service (Amazon S3)	`destinationBucketName` com um valor aleatório que começa com `awsbackup-restore-test-`
	
	`encrypted` com valor definido como `true`
	
	`encryptionType` com valor definido como `SSE-S3`
	
	`newBucket` com valor definido como `true`
		`encryptionType`
		
		`kmsKey`

Restaurar a validação do teste

Você tem a opção de criar uma validação orientada por eventos que é executada quando um trabalho de teste de restauração é concluído.

Primeiro, crie um fluxo de trabalho de validação com qualquer destino suportado pela Amazon EventBridge, como AWS Lambda. Em segundo lugar, adicione uma EventBridge regra que detecte o trabalho de restauração atingindo o status`COMPLETED`. Em terceiro lugar, crie um plano de teste de restauração (ou deixe um existente ser executado conforme programado). Por fim, após a conclusão do teste de restauração, monitore os registros do fluxo de trabalho de validação para garantir que ele foi executado conforme o esperado (depois que a validação for executada, um status de validação será exibido no AWS Backup console).

1. Configurar fluxo de trabalho de validação

   Você pode configurar um fluxo de trabalho de validação usando o Lambda ou qualquer outro destino suportado pelo. EventBridge Por exemplo, se você estiver validando um teste de restauração contendo uma instância do Amazon EC2, você pode incluir um código que efetue ping em um endpoint de verificação de integridade.

Você pode usar os detalhes do evento para determinar quais recursos devem ser validados.

Você pode usar uma camada Lambda personalizada para usar o SDK mais recente (já que ainda não `PutRestoreValidationResult` está disponível por meio do Lambda SDK).

Aqui está uma amostra:

```
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. Adicionar uma EventBridge regra

   Crie uma EventBridge regra que escute o `COMPLETED`evento do trabalho de restauração.

   Opcionalmente, você pode filtrar eventos por tipo de recurso ou restaurar o ARN do plano de teste. Defina a meta dessa regra para invocar o fluxo de trabalho de validação que você definiu na Etapa 1. Exemplo:

```
{
  "source":[
    "aws.backup"
  ],
  "detail-type":[
```

```
    "Restore Job State Change"
  ],
  "detail":{
    "resourceType":[
      "..."
    ],
    "restoreTestingPlanArn":[
      "..."
    ],
    "status":[
      "COMPLETED"
    ]
  }
}
```

3. Deixe o plano de teste de restauração ser executado e concluído

   O plano de teste de restauração será executado de acordo com a programação que você configurou.

   Consulte Criar um plano de teste de restauração se você ainda não tiver um ou Atualizar um plano de teste de restauração se desejar alterar as configurações.

4. Monitore os resultados

   Depois que um plano de teste de restauração for executado conforme programado, você poderá verificar os registros do seu fluxo de trabalho de validação para garantir que ele foi executado corretamente.

   Você pode chamar a API `PutRestoreValidationResult` para publicar os resultados, que serão então visualizados no AWS Backup console e por meio de chamadas de AWS Backup API que descrevem e listam trabalhos de restauração, como `DescribeRestoreJob` ou`ListRestoreJob`.

   Depois que um status de validação é definido, ele não pode ser alterado.

Visualizar uma lista de backups

Você pode ver uma lista dos seus backups usando o AWS Backup console ou programaticamente.

Tópicos

Listar backups por recurso protegido no console

Siga estas etapas para exibir uma lista de backups de um recurso específico no console do AWS Backup .

1. Faça login no AWS Management Console e abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, escolha Recursos protegidos.
3. Escolha um recurso protegido na lista para visualizar a lista de backups. Somente os recursos que foram copiados por AWS Backup estão listados em Recursos protegidos.

É possível visualizar os backups do recurso. Nesta tela, você também pode escolher um backup e restaurá-lo.

Listar backups por cofre de backup no console

Siga estas etapas para exibir uma lista de backups organizados em um cofre de backup.

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Cofres de Backup.
3. Na seção Backups, visualize a lista de todos os backups organizados neste cofre de backup. Nessa visualização, é possível classificar os backups por qualquer um dos cabeçalhos de coluna (incluindo status), bem como selecionar um backup para restaurá-lo, editá-lo ou excluí-lo.

Listar backups de forma programática

É possível listar os backups de forma programática usando as operações `ListRecoveryPoint` da API:

- `ListRecoveryPointsByBackupVault`
- `ListRecoveryPointsByResource`

Por exemplo, o comando a seguir AWS Command Line Interface (AWS CLI) lista todos os seus backups com o `EXPIRED` status:

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

Você pode usar o AWS Backup Audit Manager para auditar a conformidade de suas AWS Backup políticas em relação aos controles definidos por você. Controle é um procedimento criado para auditar a conformidade de um requisito de backup, como a frequência ou o período de retenção do backup.

AWS Backup O Audit Manager ajuda você a responder perguntas como:

- “Estou fazendo backup de todos os meus recursos?”
- “Todos os meus backups são criptografados?”
- “Meus backups estão ocorrendo diariamente?”

Você pode usar o AWS Backup Audit Manager para encontrar atividades e recursos de backup que ainda não estejam em conformidade com os controles que você definiu. Observe que somente os recursos ativos serão incluídos quando os controles avaliarem a conformidade dos recursos. Por exemplo, uma instância do Amazon EC2 em um estado de execução será avaliada. Uma instância do EC2 em um estado interrompido não será incluída na avaliação de conformidade.

Você também pode usá-lo para gerar automaticamente uma trilha de auditoria de relatórios diários e sob demanda para fins de governança de backup.

As etapas a seguir fornecem uma visão geral de como usar o AWS Backup Audit Manager. Para obter orientações detalhadas, escolha um dos tópicos no final desta página.

1. Crie frameworks que contenham um ou mais modelos de controle de governança. As perguntas anteriores são exemplos de três modelos de controle de governança. É possível personalizar os parâmetros de alguns modelos de controle de governança. Por exemplo, você pode personalizar o último controle para perguntar: “Meus backups estão ocorrendo semanalmente?” em vez de diariamente.
2. Visualize sua framework para ver quantos de seus recursos estão em conformidade (ou não) com os controles que você definiu nessa framework.
3. Crie relatórios sobre seu status de backup e conformidade. Armazene esses relatórios como evidência demonstrável de suas práticas de conformidade ou para identificar atividades e recursos de backup individuais que ainda não estejam em conformidade.

AWS Backup O Audit Manager gera automaticamente um novo relatório para você a cada 24 horas e o publica no Amazon S3. Também é possível gerar relatórios sob demanda.

> **Note**
>
> Antes de criar sua primeira framework relacionada à conformidade, é necessário ativar o rastreamento de recursos. Isso permite AWS Config rastrear seus AWS Backup recursos. Para obter documentação técnica sobre como gerenciar o rastreamento de recursos, consulte Configuração AWS Config com o console no Guia do AWS Config desenvolvedor. As cobranças serão aplicadas quando você ativar o rastreamento de recursos. Para obter informações sobre controle de recursos, preços e cobrança para o AWS Backup Audit Manager, consulte Medição, custos e cobrança.

Tópicos

Trabalhar com frameworks de auditoria

Uma framework é uma coleção de controles podem ser utilizados para avaliar suas práticas de backup. É possível usar controles personalizáveis predefinidos para definir suas políticas, você pode avaliar se as suas práticas de backup estão em conformidade com as suas políticas. Você também pode configurar relatórios diários automáticos para obter informações sobre o status de conformidade de suas frameworks.

Cada estrutura se aplica a uma única conta Região da AWS e. Você pode implantar no máximo 15 estruturas por conta por região. Não é possível implantar frameworks duplicadas (frameworks que contêm os mesmos controles e parâmetros).

Há dois tipos diferentes de frameworks:

- A framework do AWS Backup (recomendada): use a framework do AWS Backup para implantar todos os controles disponíveis para monitorar sua atividade, cobertura e recursos de backup em relação às melhores práticas que recomendamos.
- Uma framework personalizada que você define: use uma framework personalizada para escolher um ou mais controles específicos e personalizar os parâmetros de controle.

Tópicos

Escolher seus controles

A tabela a seguir lista os controles do AWS Backup Audit Manager, seus parâmetros personalizáveis e seus tipos de recursos de AWS Config gravação. Todo controle requer o tipo de recurso de gravação do `AWS Config: resource compliance` porque esse tipo registra o status de conformidade.

Controles disponíveis

Nome do controle	Descrição do controle	Parâmetros personalizáveis	AWS Config tipo de recurso de gravação
Recursos de backup protegidos por um plano de backup	Avalia se os recursos estão protegidos por um plano de backup.	Nenhum	`AWS Backup: backup selection`
O plano de backup tem frequência	Avalia se a frequência de backup é de pelo menos [1 dia] e	Frequência de backup; período de retenção	`AWS Backup: backup plans`

Nome do controle	Descrição do controle	Parâmetros personalizáveis	AWS Config tipo de recurso de gravação
mínima e retenção mínima	o período de retenção é de pelo menos [35 dias].		
Os cofres impedem a exclusão manual dos pontos de recuperação	Avalia se os cofres de backup não permitem a exclusão manual de pontos de recuperação, exceto por determinadas funções AWS Identity and Access Management (IAM). Por padrão, não há exceções de perfil do IAM. Também não há exceções de função do IAM quando você implanta esse controle com a AWS Backup estrutura.	Até cinco perfis do IAM que permitem a exclusão manual de pontos de recuperação	`AWS Backup: backup vaults`
Os pontos de recuperação são criptografados	Avalia se os pontos de recuperação estão criptografados.	Nenhum	`AWS Backup: recovery points`
Retenção mínima estabelecida para o ponto de recuperação	Avalia se o período de retenção do ponto de recuperação é de pelo menos [35 dias].	Período de retenção do ponto de recuperação	`AWS Backup: recovery points`

Nome do controle	Descrição do controle	Parâmetros personalizáveis	AWS Config tipo de recurso de gravação
A cópia de backup entre regiões está programada	Avalia se um recurso está configurado para criar cópias de seus backups em outra Região da AWS.	Região da AWS	`AWS Backup: backup selection`
Uma cópia de backup entre contas está programada	Avalia se um recurso tem uma cópia de backup entre contas configurada.	AWS ID da conta	`AWS Backup: backup selection`
Os backups são protegidos pelo AWS Backup Vault Lock	Avalia se um recurso está configurado para ter backups em um cofre de backup bloqueado.	Dias mínimos de retenção; dias máximos de retenção	`AWS Backup: backup selection`
O último ponto de recuperação foi criado	Avalia se um ponto de recuperação foi criado dentro do prazo especificado.	Valor em horas [de 1 às 744] ou dias [de 1 a 31].	`AWS Backup recovery points`
Tempo de restauração para recursos cumpre a meta	Avalia se o trabalho de testes de restauração foi concluído dentro do tempo de restauração previsto.	Valor em minutos	Nenhum

Para obter informações detalhadas sobre esses controles, consulte Controles e remediação.

Para ver uma lista dos recursos AWS Backup compatíveis que não oferecem suporte a todos os controles, consulte a seção AWS Backup Audit Manager da Disponibilidade de recursos por recurso tabela.

> **Note**
>
> Se você não quiser usar nenhum dos controles anteriores, ainda poderá usar o AWS Backup Audit Manager para criar relatórios diários de suas tarefas de backup, cópia e restauração. Consulte Trabalhar com relatórios de auditoria.

Ativar o rastreamento de recursos

Antes de criar sua primeira framework relacionada à conformidade, é necessário ativar o rastreamento de recursos. Isso permite AWS Config rastrear seus AWS Backup recursos. Para obter documentação técnica sobre como gerenciar o rastreamento de recursos, consulte Configuração AWS Config com o console no Guia do AWS Config desenvolvedor.

As cobranças serão aplicadas quando você ativar o rastreamento de recursos. Para obter informações sobre controle de recursos, preços e cobrança para o AWS Backup Audit Manager, consulte Medição, custos e cobrança.

Tópicos

- Ativar o rastreamento de recursos usando o console
- Ativar o rastreamento de recursos usando a AWS Command Line Interface (AWS CLI)
- Ativar o rastreamento de recursos usando um modelo do AWS CloudFormation

Ativar o rastreamento de recursos usando o console

Como ativar o rastreamento de recursos usando o console:

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, em Audit Manager, escolha Frameworks.
3. Ative o rastreamento de recursos escolhendo Gerenciar rastreamento de recursos.
4. Escolha Ir para AWS Config configurações.
5. Escolha Ativar ou desativar a gravação.
6. Escolha Habilitar a gravação para todos os tipos de recursos a seguir ou escolha habilitar a gravação para alguns tipos de recursos. Consulte Controles e correções do AWS Backup Audit Manager para saber quais tipos de recursos são necessários para seus controles.

- `AWS Backup: backup plans`
- `AWS Backup: backup vaults`
- `AWS Backup: recovery points`
- `AWS Backup: backup selection`

> **Note**
>
> AWS Backup O Audit Manager `AWS Config: resource compliance` exige todos os controles.

7. Escolha Fechar.
8. Aguarde até que o banner azul com o texto Ativando o rastreamento de recursos faça a transição para o banner verde com o texto O rastreamento de recursos está ativado.

Você pode verificar se ativou o rastreamento de recursos e, em caso afirmativo, quais tipos de recursos você está gravando, em dois lugares no AWS Backup console. No painel de navegação esquerdo:

- Escolha Frameworks e, em seguida, escolha o texto em Status do gravador do AWS Config .
- Escolha Configurações e, depois, escolha o texto em Status do gravador do AWS Config .

Ativar o rastreamento de recursos usando a AWS Command Line Interface (AWS CLI)

Se você ainda não embarcou no AWS Config, talvez seja mais rápido fazer a integração usando o. AWS CLI

Como ativar o rastreamento de recursos usando a AWS CLI:

1. Digite o comando a seguir para determinar se você já ativou o gravador do AWS Config .

```
$ aws configservice describe-configuration-recorders
```

   a. Se a sua lista de `ConfigurationRecorders` estiver vazia como desta forma:

```
{
  "ConfigurationRecorders": []
```

```
}
```

Seu gravador não está habilitado. Continue para a etapa 2 para criar o gravador.

b. Se já tiver habilitado a gravação para todos os recursos, a saída de `ConfigurationRecorders` ficará assim:

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
      "name":"default"
    }
  ]
}
```

Uma vez que você tenha habilitado todos os recursos, você já terá ativado o rastreamento de recursos. Você não precisa concluir o restante desse procedimento para usar o AWS Backup Audit Manager.

c. Se a `ConfigurationRecorders` não estiver vazia, mas você não tiver habilitado a gravação para todos os recursos, adicione recursos de backup ao seu gravador existente usando o comando a seguir. Depois disso, prossiga para a etapa 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. Crie um AWS Config gravador com os tipos de recursos do 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. Descreva seu AWS Config gravador.

```
$ aws configservice describe-configuration-recorders
```

Verifique se ele tem os tipos de recursos do AWS Backup Audit Manager comparando sua saída com a seguinte saída esperada.

```
{
  "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. Crie um bucket do Amazon S3 como destino para armazenar os arquivos de AWS Config configuração.

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. Use *policy.json* para conceder AWS Config permissão para acessar seu bucket. Veja o exemplo de *policy.json* a seguir.

```
$ 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. Configure seu bucket como um canal AWS Config de entrega

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. Ativar AWS Config gravação

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name default
```

8. Verifique se `"FrameworkStatus":"ACTIVE"` na última linha de sua saída `DescribeFramework` da seguinte forma:

```
$ 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"
}
```

Ativar o rastreamento de recursos usando um modelo do AWS CloudFormation

Para um AWS CloudFormation modelo que ativa o rastreamento de recursos, consulte Usando o AWS Backup Audit Manager com AWS CloudFormation.

Criar frameworks usando o console do AWS Backup

Depois de ativar o rastreamento de recursos, crie uma framework usando as etapas a seguir.

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, selecione Frameworks.
3. Escolha Criar framework.
4. Em Nome da framework, insira um nome exclusivo. Esse nome de framework deve ter entre 1 e 256 caracteres, começando com uma letra, e consiste em letras (a-z, A-Z), números (0-9) e sublinhados (_).
5. (Opcional) Insira uma Descrição da framework.
6. Em Controles, seus controles ativos serão exibidos. Por padrão, todos os controles elegíveis para um recurso são listados.

   Para alterar quais controles estão ativos, clique em Editar controles.

   a. A primeira caixa de seleção indica se o controle está ativado. Para desativar um controle, desmarque a caixa.
   b. Em Escolher recursos a serem avaliados, você poderá selecionar como escolher recursos, seja por tipo, por tags ou por um único recurso.

   A lista de Controles do AWS Backup Audit Manager descreve as opções de personalização de cada controle.
7. (Opcional) Marque a framework escolhendo Adicionar nova tag. Você pode usar tags para pesquisar e filtrar as frameworks ou monitorar seus custos.

8. Escolha Criar framework.

AWS Backup O Audit Manager pode levar alguns minutos para criar a estrutura.

Se o erro `AlreadyExists` ocorrer, isso indica que já existe uma framework com os mesmos controles e parâmetros. Para criar uma framework com êxito, pelo menos um controle ou parâmetro deve ser diferente das frameworks existentes.

Criação de estruturas usando a API AWS Backup

A tabela a seguir contém exemplos de solicitações de API CreateFramework para cada controle, junto com exemplos de respostas de API às solicitações DescribeFramework correspondentes. Para trabalhar com o AWS Backup Audit Manager de forma programática, você pode consultar esses trechos de código.

Controle	Solicitação **CreateFramework**	Resposta **DescribeFramework**
`Backup resources are protected by a backup plan`	`{"FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [ {"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["RDS"] // Evaluate only RDS instances } } ],`	`{"FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes":`

Controle	Solicitação **CreateFramework**	Resposta **DescribeFramework**
	"IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }	["RDS"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }

Controle	Solicitação **CreateFramework**	Resposta **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": {

Controle	Solicitação **CreateFramework**	Resposta **DescribeFramework**
	"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }	"Tags": {"key1": "prod"} } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }

Controle	Solicitação **CreateFramework**	Resposta **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

Controle	Solicitação **CreateFramework**	Resposta **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>

Controle	Solicitação **CreateFramework**	Resposta **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":

Controle	Solicitação **CreateFramework**	Resposta **DescribeFramework**
		{"key1": "foo"} }

Backup recovery points are encrypted	{"FrameworkName":
	"Control5",
	"FrameworkDescription": "This is a test framework",
	"FrameworkControls":
	[
	{"ControlName":
	"BACKUP_RECOVERY_POINT_ENCRYPTED",
	"ControlInputParameters":
	[],
	"ControlScope":
	{} // Default scope (no scope input) is all recovery points
	}
	],
	"IdempotencyToken":
	"Control5",
	"FrameworkTags":
	{"key1": "foo"}
	}
		{"FrameworkName":
		"Control5",
		"FrameworkArn":
		"arn:aws:backup:us-east-1:123456789012:framework/Control7-7e7655ae-1e31-45cb-96a0-4f43d8c19642",
		"FrameworkDescription": "This is a test framework",
		"FrameworkControls":
		[
		{"ControlName":
		"BACKUP_RECOVERY_POINT_ENCRYPTED",
		"ControlInputParameters":
		[],
		"ControlScope": {}
		}
		],
		"CreationTime":
		1516925490,
		"DeploymentStatus":
		"Active",
		"FrameworkStatus":
		"Completed",
		"IdempotencyToken":
		"Control5",
		"FrameworkTags":
		{"key1": "foo"}
		}

Controle	Solicitação **CreateFramework**	Resposta **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"} }

Controle	Solicitação **CreateFramework**	Resposta **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"} }

Controle	Solicitação **CreateFramework**	Resposta **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"} }

Controle	Solicitação **CreateFramework**	Resposta **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"} }

Controle	Solicitação **CreateFramework**	Resposta **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"} }

Controle	Solicitação **CreateFramework**	Resposta **DescribeFramework**
	`}`	

Visualizar o status de conformidade da framework

Depois de criar uma framework de auditoria, ela será exibida na tabela Frameworks. Você pode visualizar essa tabela escolhendo Frameworks no painel de navegação esquerdo do AWS Backup console. Para visualizar os resultados da auditoria de sua framework, escolha o Nome da framework. Isso levará você à página Detalhes da framework, que tem duas seções: Resumo e Controles.

A seção Resumo lista os seguintes status da esquerda para a direita:

- O status de conformidade é o status geral de conformidade da framework de auditoria, conforme determinado pelo status de conformidade de cada um de seus controles. O status de conformidade de cada controle é determinado pelo status de conformidade de cada recurso que ele avalia.

  O status de conformidade da framework será `Compliant` somente se todos os recursos no escopo de suas avaliações de controle tiverem sido aprovados nessas avaliações. Se houver falha em um ou mais recursos em uma avaliação de controle, o status de conformidade será `Non-Compliant`. Para obter informações sobre como encontrar os recursos que não estejam em conformidade, consulte Encontrar recursos que não estão em conformidade. Para obter informações sobre como colocar seus recursos em conformidade, consulte a seção de correções Controles e correções do AWS Backup Audit Manager.
- O status da framework se refere a se você ativou o rastreamento de recursos para todos os seus recursos. Os possíveis status são:
  - `Active` quando a gravação está ativada para todos os recursos que a framework avalia.
  - `Partially active` quando a gravação está desativada para pelo menos um recurso que a framework avalia.
  - `Inactive` quando a gravação está desativada para todos os recursos que a framework avalia.
  - `Unavailable`quando o AWS Backup Audit Manager não consegue validar o status da gravação no momento.

  Como corrigir um status **`Partially active`** ou **`Inactive`**

  1. Selecione Usuário no painel de navegação esquerdo.

2. Selecione Gerenciar rastreamento de recursos.
3. Siga as instruções na janela pop-up para ativar a gravação que não estava habilitada anteriormente para seus tipos de recursos.

Para obter mais informações sobre quais tipos de recursos exigem rastreamento de recursos com base nos controles que você incluiu em suas frameworks, consulte o componente do recurso de Controles e correções do AWS Backup Audit Manager.

- O status de implantação se refere ao status de implantação da framework. Esse status geralmente deve ser `Completed`, mas também pode ser `Create in progress`, `Update in progress`, `Delete in progress` e `Failed`.
  - Um status de `Failed` significa que a framework não foi implantada corretamente. Exclua a framework e recrie-a por meio do console do AWS Backup ou da API do AWS Backup.
- Os controles em conformidade mostram uma contagem de controles da framework com todas as avaliações aprovadas.
- Os controles que não estão em conformidade mostram uma contagem de controles da framework com pelo menos uma avaliação não aprovada.

A seção Controles, mostra as seguintes informações:

- O status do controle se refere ao status de conformidade de cada controle. Um controle pode ser`Compliant`, que significa que todos os recursos passaram nessa avaliação; `Non-compliant`, que significa que pelo menos um recurso não passou nessa avaliação ou `Insufficient data`, que significa que o controle não encontrou recursos dentro do escopo da avaliação para avaliar.
- O escopo da avaliação pode limitar cada controle a um ou mais tipos de recursos, um ID de recurso ou uma chave de tag e valor de tag, com base em como você personalizou o controle ao criar a framework de auditoria. Se todos os campos estiverem vazios (conforme mostrado por um traço, “-”), o controle avaliará todos os recursos aplicáveis.

Encontrar recursos que não estão em conformidade

AWS Backup O Audit Manager ajuda você a descobrir quais recursos não estão em conformidade de duas maneiras.

- Ao Visualizar o status de conformidade da framework, escolha o nome do controle na seção Detalhes. Isso leva você ao AWS Config console, onde você pode ver uma lista dos seus `Non-Compliant` recursos.
- Depois de criar um plano de relatório com o modelo de conformidade de recursos que inclui sua framework, você poderá visualizar seu relatório para identificar todos os recursos do `Non-Compliant` em todos os seus controles.

  Além disso, o `Resource compliance report` mostra a última vez que o AWS Backup Audit Manager avaliou cada um dos seus controles pela última vez.

Atualizar frameworks de auditoria

É possível atualizar a descrição, os controles e os parâmetros de uma framework de auditoria existente.

Como atualizar uma framework existente

1. No painel de navegação esquerdo AWS Backup do console, escolha Frameworks.
2. Escolha a framework que você deseja editar pelo Nome da framework.
3. Selecione a opção Editar.

Excluir frameworks de auditoria

Como excluir uma framework existente

1. No painel de navegação esquerdo AWS Backup do console, escolha Frameworks.
2. Escolha a framework que você deseja excluir pelo Nome da framework.
3. Escolha Excluir.
4. Digite o nome da framework e escolha Excluir framework.

Trabalhar com relatórios de auditoria

AWS Backup Os relatórios do Audit Manager são evidências geradas automaticamente de sua AWS Backup atividade, como:

- Quais trabalhos de backup foram concluídos e quando

- Quais recursos tiveram backup

Há dois tipos de relatório. Ao criar um relatório, escolha o tipo a ser criado.

Um tipo é o relatório de trabalhos, que mostra os trabalhos concluídos nas últimas 24 horas e todos os trabalhos ativos. Os relatórios de trabalhos não exibem o status de `completed with issues`. Para encontrar esse status, você pode filtrar `Completed` trabalhos com uma ou mais mensagens de status. AWS Backup só incluirá uma mensagem de status como parte do status de um `Completed` trabalho se a mensagem exigir atenção ou ação.

O segundo tipo de relatório é o relatório de conformidade. Os relatórios de conformidade podem monitorar os níveis de recursos ou os diferentes controles em vigor.

AWS Backup O Audit Manager entrega um relatório diário em seu bucket do Amazon S3. Se o relatório for para a região e a conta atuais, você poderá optar por receber o relatório no formato CSV ou JSON. Caso contrário, o relatório estará disponível no formato CSV. O tempo do relatório diário pode variar ao longo de várias horas porque o AWS Backup Audit Manager realiza a randomização para manter seu desempenho. Também é possível gerar um relatório sob demanda a qualquer momento.

Todos os titulares de conta podem criar relatórios entre regiões. Os titulares de contas administrativas e administrativas delegadas também podem criar relatórios entre contas.

Você pode ter no máximo 20 planos de relatórios por Conta da AWS.

> **Note**
>
> Recursos como o RDS, que não têm a capacidade de mostrar bytes incrementais de dados de um backup específico, exibirão o valor `backupSizeInBytes` como 0.

Para permitir que o AWS Backup Audit Manager crie relatórios diários ou sob demanda, você deve primeiro criar um plano de relatório a partir de um modelo de relatório.

Tópicos

- Escolher o modelo de relatório
- Criar planos de relatório usando o console do AWS Backup
- Criação de planos de relatórios usando a AWS Backup API
- Criar relatórios sob demanda

- Visualizar relatórios de auditoria
- Atualizar planos de relatórios
- Excluir planos de relatório

Escolher o modelo de relatório

Um modelo de relatório define as informações que seu plano de relatório inclui no relatório. Quando você automatiza seus relatórios usando um plano de relatórios, o AWS Backup Audit Manager fornece relatórios das 24 horas anteriores. AWS Backup O Audit Manager cria esses relatórios entre 1h e 5h UTC. Ele oferece os seguintes modelos de relatório:

Modelos de relatório de backup

Modelos de relatório de backup. Esses modelos fornecem atualizações diárias sobre seus trabalhos de backup, restauração ou cópia. Você pode usar esses relatórios para monitorar sua postura operacional e identificar quaisquer falhas que possam precisar de medidas adicionais. A tabela a seguir lista o nome de cada modelo de relatório de backup e sua saída de exemplo.

Modelo de relatório de backup	Relatório de exemplo em 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",

Modelo de relatório de backup	Relatório de exemplo em formato JSON


```
      "backupRuleId": "ab88bbf8-
ff4e-4f1b-92e7-e13d3e65dcfb",
      "creationDate": "2021-07-
14T23:53:47.229Z",
      "completionDate": "2021-07-
15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:
ec2:us-west-2::image/ami-03
0cafb98e5a6dcdf",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 858993459
2,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-vault:Default",
      "iamRoleArn": "arn:aws:
iam::112233445566:role/service-
role/AWSBackupDefaultServiceRole"
    }
  ]
}
```

Modelo de relatório de backup	Relatório de exemplo em 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"
	    }

Modelo de relatório de backup	Relatório de exemplo em formato JSON
	<pre>] }</pre>

RESTORE_JOB_REPORT	<pre>{
	  "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"
	    }
	  ]
	}</pre>

Modelos de relatórios de conformidade

Os modelos de relatórios de conformidade fornecem relatórios diários sobre a conformidade de suas atividades e recursos de backup em relação aos controles que você definiu em uma ou mais frameworks. Se o status de conformidade de uma de suas frameworks for `Non-compliant`, revise um relatório de conformidade para identificar os recursos que não estão em conformidade.

Tipos de modelos de relatórios de conformidade

- `Control compliance report` ajuda você a rastrear o status de conformidade dos controles que você definiu nas frameworks.
- `Resource compliance report` ajuda você a monitorar o status de conformidade de seus recursos em relação aos controles definidos nas frameworks. Esses relatórios incluem resultados de avaliação detalhados, incluindo informações de identificação sobre recursos que não estão em conformidade que podem ser usadas para identificar e corrigir esses recursos.

A tabela a seguir mostra algumas saídas de exemplo de um relatório de conformidade.

Modelo de relatório de conformidade	Relatório de exemplo em 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",

Modelo de relatório de conformidade	Relatório de exemplo em 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
\"}"
    }
  ]
}
```

Modelo de relatório de conformidade	Relatório de exemplo em 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"
	    }
	  ]
	}

Criar planos de relatório usando o console do AWS Backup

Há dois tipos de relatório: Um tipo é o relatório de trabalhos, que mostra os trabalhos concluídos nas últimas 24 horas e todos os trabalhos ativos. O segundo tipo de relatório é o relatório de conformidade. Os relatórios de conformidade podem monitorar os níveis de recursos ou os diferentes controles em vigor. Ao criar um relatório, escolha o tipo de relatório a ser criado.

OBSERVAÇÃO: dependendo do seu tipo de conta, a tela do console pode variar. Somente contas de gerenciamento verão a funcionalidade de várias contas.

Semelhante a um plano de backup, você cria um plano de relatório para automatizar a criação de seus relatórios e definir seu bucket do Amazon S3 de destino. Um plano de relatório exige que você tenha um bucket do S3 para receber os relatórios. Para obter instruções sobre como configurar um novo bucket do S3, consulte Etapa 1: Criar seu primeiro bucket do S3 no Guia do usuário do Amazon Simple Storage Service.

Para criar seu plano de relatório no AWS Backup console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Relatórios.
3. Escolha Criar grupo de relatórios.
4. Escolha um dos modelos de relatório na lista suspensa.
5. Insira um nome exclusivo para o plano de relatório. Esse nome deve ter entre 1 e 256 caracteres, começando com uma letra, e consistir em letras (a-z, A-Z), números (0-9) e sublinhados (_).
6. (Opcional) Insira uma Descrição do plano de relatório.
7. Modelos de relatório de conformidade para somente uma conta. Escolha uma ou mais frameworks sobre as quais gerar o relatório. É possível adicionar no máximo 1.000 frameworks a um plano de relatório.

    1. Escolha sua AWS região usando o menu suspenso.
    2. Escolha uma framework dessa região usando o menu suspenso.
    3. Escolha Adicionar framework.
8. (Opcional) Para adicionar tags ao plano de relatório, escolha Adicionar tags ao plano de relatório.
9. Se estiver usando uma conta de gerenciamento, você poderá especificar quais contas deseja incluir nesse plano de relatório. Você poderá selecionar Somente minha conta, que

gerará relatórios somente sobre a conta na qual você está conectado no momento. Ou você pode selecionar Uma ou mais contas em minha organização (disponível para contas de gerenciamento e de administrador delegado).

10. (Se você estiver criando um relatório de conformidade somente para uma região, ignore essa etapa). É possível selecionar quais regiões incluir no relatório. Clique no menu suspenso para mostrar as regiões disponíveis para você. Selecione Todas as regiões disponíveis ou as regiões de sua preferência.

    - A caixa de seleção Incluir novas regiões quando elas forem incorporadas ao Backup Audit Manager fará com que novas regiões sejam incluídas em seus relatórios quando estiverem disponíveis.

11. Escolha o formato de arquivo do seu relatório. Todos os relatórios podem ser exportados no formato CSV. Além disso, os relatórios de uma única região podem ser exportados no formato JSON.
12. Escolha o Nome do bucket do S3 usando a lista suspensa.
13. (Opcional) Insira um prefixo de bucket.

    AWS Backup entrega sua conta corrente, a região atual se reporta para`s3://your-bucket-name`/prefix/Backup/`accountID`/`Region`/year/month/day/report-name.

    AWS Backup entrega seus relatórios de várias contas para `s3://your-bucket-name`/prefix/Backup/crossaccount/`Region`/year/month/day/report-name

    AWS Backup entrega seus relatórios interregionais para `s3://your-bucket-name`/prefix/Backup/`accountID`/crossregion/year/month/day/report-name
14. Escolha Criar grupo de relatórios.

Em seguida, você deve permitir que seu bucket do S3 receba relatórios do AWS Backup. Depois de criar um plano de relatório, o AWS Backup Audit Manager gera automaticamente uma política de acesso ao bucket do S3 para você aplicar.

Se você criptografar seu bucket usando uma chave KMS personalizada, a política de chaves KMS deverá atender aos seguintes requisitos:

- O `Principal` atributo deve incluir o `AWSServiceRolePolicyForBackupReports`ARN da função vinculada ao serviço do Backup Audit Manager.

- O `Action` atributo deve incluir `kms:GenerateDataKey` e`kms:Decrypt`, no mínimo.

A política AWSServiceRolePolicyForBackupReportstem essas permissões.

Como visualizar e aplicar essa política de acesso ao seu bucket do S3

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Relatórios.
3. Em Nome do plano de relatório, selecione um plano de relatório escolhendo seu nome.
4. Selecione a opção Editar.
5. Escolha Exibir política de acesso para o bucket do S3. Também é possível usar a política no final deste procedimento.
6. Escolha Copiar permissões.
7. Escolha Editar política de bucket. Observe que até que o relatório de backup seja criado pela primeira vez, a função vinculada ao serviço mencionada na política de bucket do S3 ainda não existirá, resultando no erro “Principal inválido”.
8. Copie as permissões na Política.

Política de bucket de exemplo

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

Se você usar uma personalização AWS Key Management Service para criptografar seu bucket do S3 de destino que armazena os relatórios, inclua as seguintes ações em sua política:

```
      "Action":[
        "kms:GenerateDataKey",
        "kms:Encrypt"
      ],
      "Resource":[
        "*"
      ],
```

Criação de planos de relatórios usando a AWS Backup API

Também é possível trabalhar com planos de relatórios de forma programática.

Há dois tipos de relatório: Um tipo é o relatório de trabalhos, que mostra os trabalhos concluídos nas últimas 24 horas e todos os trabalhos ativos. O segundo tipo de relatório é o relatório de conformidade. Os relatórios de conformidade podem monitorar os níveis de recursos ou os diferentes controles em vigor. Ao criar um relatório, escolha o tipo de relatório a ser criado.

Semelhante a um plano de backup, você cria um plano de relatório para automatizar a criação de seus relatórios e definir seu bucket do Amazon S3 de destino. Um plano de relatório exige que você tenha um bucket do S3 para receber os relatórios. Para obter instruções sobre como configurar um novo bucket do S3, consulte Etapa 1: Criar seu primeiro bucket do S3 no Guia do usuário do Amazon Simple Storage Service.

Se você criptografar seu bucket usando uma chave KMS personalizada, a política de chaves KMS deverá atender aos seguintes requisitos:

- O `Principal` atributo deve incluir o `AWSServiceRolePolicyForBackupReports`ARN da função vinculada ao serviço do Backup Audit Manager.

- O `Action` atributo deve incluir `kms:GenerateDataKey` e`kms:Decrypt`, no mínimo.

A política AWSServiceRolePolicyForBackupReportstem essas permissões.

Para relatórios de conta única e região única, use a sintaxe a seguir para chamar 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"
}
```

Quando você chama DescribeReportPlan com o nome exclusivo de um plano de relatório, a API do AWS Backup responde com as seguintes informações:

```
{
    "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 relatórios de várias contas e várias regiões, use a sintaxe a seguir para chamar 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"
   }
}
```

Quando você chama DescribeReportPlan com o nome exclusivo de um plano de relatório, a API do AWS Backup responde com as seguintes informações para planos de várias contas e várias regiões:

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

Criar relatórios sob demanda

Você pode gerar novos relatórios conforme sua conveniência criando um relatório sob demanda com as etapas a seguir. AWS Backup O Audit Manager entrega seu relatório sob demanda para o bucket Amazon S3 que você especificou em seu plano de relatório.

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Relatórios.
3. Em Nome do plano de relatório, selecione um plano de relatório escolhendo seu nome.
4. Escolha Criar relatório sob demanda.

É possível gerar um relatório sob demanda para um plano de relatório existente.

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Relatórios.
3. Em Planos de relatório, selecione um plano de relatório clicando no botão de opção ao lado do nome do plano de relatório.
4. Clique em Ações e, depois, clique em Criar relatório sob demanda.

É possível fazer isso para vários relatórios, mesmo enquanto os relatórios estão sendo gerados.

Visualizar relatórios de auditoria

Você pode abrir, visualizar e analisar relatórios do AWS Backup Audit Manager usando os programas que você normalmente usa para trabalhar com arquivos CSV ou JSON. Observe que os relatórios de várias regiões ou de várias contas estão disponíveis somente no formato CSV.

Arquivos grandes serão divididos em vários relatórios se o tamanho total do arquivo exceder 50 MB. Se os arquivos resultantes tiverem mais de 50 MB, o AWS Backup Audit Manager criará arquivos CSV adicionais com o restante do relatório.

Como visualizar um relatório

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Relatórios.
3. Em Nome do plano de relatório, selecione um plano de relatório escolhendo seu nome.
4. Em Trabalhos de relatório, clique no link do relatório para visualizar o relatório.
5. Se o status do relatório tiver um sublinhado pontilhado, escolha-o para obter informações sobre seu relatório.
6. Escolha qual relatório exibir de acordo com o tempo de conclusão.
7. Escolha o link do S3. Isso abrirá o bucket do S3 de destino.
8. Em Nome, escolha o nome do relatório que você deseja editar.
9. Para salvar o relatório em seu computador, escolha Baixar.

Atualizar planos de relatórios

É possível atualizar a descrição de um plano de relatório existente, seu destino de entrega e o formato. Se aplicável, também é possível adicionar ou remover frameworks do plano de relatório.

Como atualizar um plano de relatório existente

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Relatórios.
3. Em Nome do plano de relatório, selecione um plano de relatório escolhendo seu nome.
4. Selecione a opção Editar.
5. É possível editar os detalhes do plano de relatório, incluindo o nome e a descrição do relatório, bem como quais contas e regiões estão incluídas nele.

Excluir planos de relatório

É possível excluir um plano de relatório existente. Quando você exclui um plano de relatório, todos os relatórios já criados por esse plano de relatório permanecerão em seu bucket do Amazon S3 de destino.

Como excluir um plano de relatório existente

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação esquerdo, escolha Relatórios.
3. Em Nome do plano de relatório, selecione um plano de relatório escolhendo seu nome.
4. Escolha Excluir.
5. Insira o nome do seu plano de relatório e escolha Excluir plano de relatório.

Usando o AWS Backup Audit Manager com AWS CloudFormation

Nós fornecemos os seguintes AWS CloudFormation modelos de amostra para sua referência:

Tópicos

- Ativar o rastreamento de recursos
- Implantar controles padrão
- Isentar perfis do IAM da avaliação de controle
- Criar um plano de relatório

Ativar o rastreamento de recursos

O modelo a seguir ativa o rastreamento de recursos conforme descrito em Ativar o controle 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
```

Implantar controles padrão

O modelo a seguir cria uma framework com os controles padrão descritos em Controles e correções do AWS Backup Audit Manager.

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
        - ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
        - ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
            - ParameterName: requiredFrequencyUnit
              ParameterValue: 'hours'
            - ParameterName: requiredFrequencyValue
              ParameterValue: '24'
          ControlScope:
            Tags:
              - Key: customizedKey
                Value: customizedValue
        - ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
          ControlInputParameters:
            - ParameterName: crossRegionList
```

```
              ParameterValue: 'eu-west-2'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
          ControlInputParameters:
            - ParameterName: crossAccountList
              ParameterValue: '111122223333'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK
        - ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
        - ControlName: RESTORE_TIME_FOR_RESOURCES_MEET_TARGET
          ControlInputParameters:
            - ParameterName: maxRestoreTime
              ParameterValue: '720'

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

Isentar perfis do IAM da avaliação de controle

O controle BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED permite que você isente até cinco perfis do IAM que ainda podem excluir os pontos de recuperação manualmente. O modelo a seguir implanta esse controle e também isenta dois perfis do 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
```

Criar um plano de relatório

O modelo a seguir cria um plano de relatório.

```
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
```

Usando o AWS Backup Audit Manager com AWS Audit Manager

AWS Backup Os controles do Audit Manager são mapeados para controles padrão predefinidos AWS Audit Manager, permitindo que você importe suas descobertas de conformidade do AWS Backup Audit Manager para seus AWS Audit Manager relatórios. Talvez você queira fazer isso para ajudar um responsável pela conformidade, gerente de auditoria ou outro colega que relata a atividade de backup como parte da postura geral de conformidade da sua organização.

Você pode importar os resultados de conformidade dos controles do AWS Backup Audit Manager para suas AWS Audit Manager estruturas. AWS Audit Manager Para permitir a coleta automática de dados dos controles do AWS Backup Audit Manager, crie um controle personalizado AWS Audit Manager usando as instruções para Personalizar um controle existente no Guia do AWS Audit Manager usuário. Ao seguir essas instruções, observe que a fonte de dados para AWS Backup controles é AWS Config.

Para obter uma lista de AWS Backup controles, consulte Como escolher seus controles.

Controles e remediação

Esta página lista os controles disponíveis para o AWS Backup Audit Manager. Você pode escolher o painel de informações correto para ver uma lista de controles e ir para um controle específico. Para comparar rapidamente os controles, consulte a tabela em Escolher seus controles. Para definir controles de forma programática, consulte os trechos de código em Criar frameworks usando a API do AWS Backup.

É possível usar até 50 controles por conta, por região. Usar o mesmo controle em duas frameworks diferentes conta como usar dois controles do limite de 50 controles.

Esta página lista cada controle com as seguintes informações:

- Descrição. Os valores entre colchetes (“[]”) são os valores padrão dos parâmetros.
- O (s) recurso (s) que o controle avalia.
- Os parâmetros do controle.
- Ocasião em que ocorre a execução do controle.
- O escopo do controle, da seguinte forma:
  - É possível especificar recursos por tipo escolhendo um ou mais serviços compatíveis com o AWS Backup.

  - Especifique um escopo de Recursos marcados com uma única chave de tag e um valor opcional.
  - É possível especificar um único recurso usando a lista suspensa Recurso único.
- Etapas de correção para colocar os recursos aplicáveis em conformidade.

Observe que somente os recursos ativos serão incluídos quando os controles avaliarem a conformidade dos recursos. Por exemplo, uma instância do Amazon EC2 em estado de execução será avaliada pelo controle O último ponto de recuperação foi criado. Uma instância do EC2 em um estado interrompido não será incluída na avaliação de conformidade.

Recursos de backup protegidos por um plano de backup

Descrição: avalia se os recursos estão protegidos por um plano de backup.

Recurso: `AWS Backup: backup selection`

Parâmetros: nenhum

Ocorre: automaticamente a cada 24 horas

Escopo:

- Recursos marcados
- Recursos por tipo (padrão)
- Recurso único

Correção: atribua os recursos a um plano de backup. o AWS Backup protege automaticamente seus recursos depois de atribuí-los a um plano de backup. Para obter mais informações, consulte Atribuir recursos a um plano de backup.

Frequência mínima e retenção mínima do plano de backup

Descrição: avalia se os planos de backup contêm pelo menos uma regra de backup com frequência de backup de pelo menos [1 dia] e o período de retenção de pelo menos [35 dias].

Recurso: `AWS Backup: backup plans`

Parâmetros:

- Frequência de backup necessária horas ou dias.
- Período de retenção obrigatório em dias, semanas, meses ou anos. Recomendamos uma retenção de armazenamento quente por um período de pelo menos uma semana AWS Backup para permitir a realização de backups incrementais sempre que possível, evitando cobranças adicionais.

Ocorre: alterações na configuração

Escopo:

- Recursos marcados
- Recurso único

Correção: atualize um plano de backup para alterar a frequência do backup, o período de retenção ou ambos. A atualização do plano de backup altera o período de retenção dos pontos de recuperação que o plano cria após a atualização.

Os cofres impedem a exclusão manual dos pontos de recuperação

Descrição: avalia se os cofres de backup não permitem a exclusão manual de pontos de recuperação, exceto por determinados perfis do IAM.

Recurso: `AWS Backup: backup vaults`

Parâmetros: os nomes dos recursos da Amazon (ARNs) de até cinco perfis do IAM permitidos a excluir manualmente os pontos de recuperação.

Ocorre: alterações na configuração

Escopo:

- Recursos marcados
- Recurso único

Correção: crie uma política de acesso baseada em recursos em um cofre de backup Para ver um exemplo de política e instruções sobre como definir uma política de acesso ao cofre de backup, consulte Negar acesso para excluir pontos de recuperação em um cofre de backup.

Os pontos de recuperação são criptografados

Descrição: avalia se os pontos de recuperação estão criptografados.

Recurso: `AWS Backup: recovery points`

Parâmetros: nenhum

Ocorre: alterações na configuração

Escopo:

- Recursos marcados

Correção: configure a criptografia para os pontos de recuperação. A forma como você configura a criptografia para pontos de AWS Backup recuperação varia de acordo com o tipo de recurso.

Você pode configurar a criptografia para tipos de recursos que oferecem suporte ao AWS Backup gerenciamento total do uso AWS Backup. Se o tipo de recurso não oferecer suporte ao AWS Backup gerenciamento completo, você deverá configurar sua criptografia de backup seguindo as instruções desse serviço, como a criptografia do Amazon EBS no Guia do Usuário do Amazon Elastic Compute Cloud. Para ver a lista de tipos de recursos que oferecem suporte ao AWS Backup gerenciamento completo, consulte a seção “ AWS Backup Gerenciamento completo” da Disponibilidade de recursos por recurso tabela.

Retenção mínima estabelecida para o ponto de recuperação

Descrição: avalia se o período de retenção do ponto de recuperação é de pelo menos [35 dias].

Recurso: `AWS Backup: recovery points`

Parâmetros: período necessário de retenção do ponto de recuperação em número de dias, semanas, meses ou anos. Recomendamos uma retenção de armazenamento quente por um período de pelo menos uma semana AWS Backup para permitir a realização de backups incrementais sempre que possível, evitando cobranças adicionais.

Ocorre: alterações na configuração

Escopo:

- Recursos marcados

Correção: altere os períodos de retenção dos seus pontos de recuperação. Para obter mais informações, consulte Editar um backup.

A cópia de backup entre regiões está programada

Descrição: avalia se um recurso está configurado para criar cópias de seus backups em outra AWS região.

Recurso: `AWS Backup: backup selection`

Parâmetros:

- Selecione o Região da AWS(s) em que a cópia de backup deve existir (opcional)
- Região

Ocorre: automaticamente a cada 24 horas

Escopo:

- Recursos marcados
- Recursos por tipo
- Recurso único

Remediação: atualize um plano de backup para alterar o Região da AWS local onde a cópia de backup deve existir.

Uma cópia de backup entre contas está programada

Descrição: avalia se um recurso está configurado para criar cópias de seus backups em outra conta. É possível adicionar até cinco contas para o controle avaliar. A conta de destino deve estar na mesma organização da conta de origem no AWS Organizations.

Recurso: `AWS Backup: backup selection`

Parâmetros:

- Selecione a (s) ID (s) da AWS conta em que a cópia de backup deve existir (opcional)
- ID da conta

Ocorre: automaticamente a cada 24 horas

Escopo:

- Recursos marcados
- Recursos por tipo
- Recurso único

Correção: atualize um plano de backup para alterar ou adicionar a (s) ID (s) da AWS conta em que a cópia deveria existir.

Os backups são protegidos pelo AWS Backup Vault Lock

Descrição: avalia se um recurso tem backups imutáveis armazenados em um cofre de backup bloqueado.

Recurso: `AWS Backup: backup selection`

Parâmetros:

- Insira os dias de retenção mínimo e máximo para o AWS Backup Vault Lock (opcional)
- Mínimo de dias de retenção
- Máximo de dias de retenção

Ocorre: automaticamente a cada 24 horas

Escopo:

- Recursos marcados
- Recursos por tipo
- Recurso único

Correção: bloqueie um cofre de backup para definir seu nome, alterar o mínimo de dias de retenção, o máximo de dias de retenção ou ambos. Também pode ser incluído `ChangeableForDays` para um bloqueio de cofre no modo de conformidade.

O último ponto de recuperação foi criado

Descrição: esse controle avalia se um ponto de recuperação foi criado dentro do período especificado (em dias ou horas).

O controle estará em conformidade se o recurso tiver um ponto de recuperação criado dentro do período especificado. O controle não estará em conformidade se um ponto de recuperação não tiver sido criado dentro do número de dias ou horas especificado.

Recurso: `AWS Backup: recovery points`

Parâmetros:

- Insira o período especificado em números inteiros, em horas ou dias.
- Os valores de `hours` podem variar de `1` a `744`.
- O valor de `days` pode variar de `1` a `31`.

Ocorre: automaticamente a cada 24 horas

Escopo:

- Recursos marcados
- Recursos por tipo
- Recurso único

Correção:

- Atualize um plano de backup para alterar o período especificado para a criação do ponto de recuperação.
- Além disso, você pode criar um backup sob demanda.

Tempo de restauração para recursos cumpre a meta

Descrição: avalia se a restauração dos recursos protegidos foi concluída dentro do tempo de restauração pretendido.

Esse controle verifica se o tempo de restauração de determinado recurso atende à duração desejada. A regra é NON_COMPLIANT se o `LatestRestoreExecutionTimeMinutes` de um recurso for maior que `maxRestoreTime` em minutos.

Parâmetros:

- `maxRestoreTime` (em minutos)

Ocorre: automaticamente a cada 24 horas

Escopo:

- Recursos marcados
- Recursos por tipo
- Recurso único

> **Note**
>
> AWS Backup não fornece nenhum contrato de nível de serviço (SLAs) para um período de restauração. Os tempos de restauração podem variar de acordo com a carga e a capacidade do sistema, mesmo para restaurações que contêm os mesmos recursos.

Gerenciando AWS Backup recursos em vários Contas da AWS

> **Note**
>
> Antes de gerenciar recursos Contas da AWS em vários estados AWS Backup, suas contas devem pertencer à mesma organização no AWS Organizations serviço.

Você pode usar o recurso de gerenciamento de várias contas AWS Backup para gerenciar e monitorar suas tarefas de backup, restauração e cópia nas Contas da AWS quais você configura. AWS OrganizationsAWS Organizationsé um serviço que oferece gerenciamento baseado em políticas para vários de uma única conta Contas da AWS de gerenciamento. Ele permite que você padronize a maneira como implementa políticas de backup, minimizando erros manuais e esforços simultaneamente. Em uma visualização centralizada, é possível identificar com facilidade recursos em todas as contas que atendam aos critérios nos quais você tenha interesse.

Se você configurar AWS Organizations, poderá configurar AWS Backup para monitorar as atividades em todas as suas contas em um só lugar. Você também pode criar uma política de backup e aplicá-la às contas selecionadas que fazem parte da sua organização e visualizar as atividades agregadas da tarefa de backup diretamente do AWS Backup console. Essa funcionalidade permite que os administradores de backup monitorem com eficiência o status do trabalho de backup em centenas de contas em toda a empresa a partir de uma única conta. Cotas do AWS Organizations são aplicáveis

Por exemplo, você define uma política de backup A que faz backups diários de recursos específicos e os mantém por sete dias. Você opta por aplicar a política de backup A em toda a organização. (Isso significa que cada conta na organização obtém essa política de backup, que cria um plano de backup correspondente visível nessa conta.) Depois, você cria uma UO chamada Finanças e decide manter seus backups por apenas 30 dias. Nesse caso, você define uma política de backup B, que substitui o valor do ciclo de vida e a anexa a essa UO Finanças. Isso significa que todas as contas na UO Finanças recebem um novo plano de backup efetivo que faz backups diários de todos os recursos especificados e os mantém por 30 dias.

Nesse exemplo, a política de backup A e a política de backup B foram mescladas em uma única política de backup, que define a estratégia de proteção para todas as contas na UO chamada Finanças. Todas as outras contas na organização permanecem protegidas pela política de backup A. A mesclagem é feita somente para políticas de backup que compartilham o mesmo nome de plano

de backup. Também é possível que a política A e a política B coexistam nessa conta sem qualquer mesclagem. É possível usar operadores avançados de mesclagem somente na visualização JSON do console. Para obter detalhes sobre a mesclagem de políticas, consulte Definir políticas, sintaxe de políticas e herança de políticas no Guia do usuário do AWS Organizations . Para referências adicionais e casos de uso, consulte o blog Gerenciando backups em grande escala em seu AWS Organizations uso AWS Backup e o tutorial em vídeo Gerenciando backups em escala em seu AWS Organizations uso AWS Backup.

Consulte Disponibilidade de recursos por AWS região para ver onde o recurso de gerenciamento de várias contas está disponível.

Para usar o gerenciamento entre contas, é necessário seguir estas etapas:

1. Crie uma conta de gerenciamento AWS Organizations e adicione contas na conta de gerenciamento.
2. Ative o recurso de gerenciamento de várias contas no AWS Backup.
3. Crie uma política de backup para ser aplicada a todos os Contas da AWS usuários da sua conta de gerenciamento.

> **Note**
>
> Para planos de backup gerenciados pelo Organizations, as configurações de inclusão de recurso na conta de gerenciamento substituem as configurações em uma conta de membro, mesmo que uma ou mais contas de administrador delegado estejam configuradas. As contas de administrador delegado são contas de membro com recursos aprimorados e não podem substituir as configurações como uma conta de gerenciamento.

4. Gerencie trabalhos de backup, restauração e cópia em todos os seus Contas da AWS.

Tópicos

- Criar uma conta de gerenciamento no Organizations
- Habilitar o gerenciamento entre contas
- Administrador delegado
- Como criar uma política de backup
- Monitorar atividades em várias Contas da AWS

- Regras de inclusão de recursos
- Definir políticas, sintaxe de políticas e herança de políticas

Criar uma conta de gerenciamento no Organizations

Primeiro, você deve criar sua organização e configurá-la com as contas AWS dos membros AWS Organizations.

Para criar uma conta de gerenciamento AWS Organizations e adicionar contas

- Para obter instruções, consulte Tutorial: Criar e configurar uma organização no Guia do usuário do AWS Organizations .

Habilitar o gerenciamento entre contas

Antes de usar o gerenciamento de várias contas AWS Backup, você precisa ativar o recurso (ou seja, ativá-lo). Depois que o recurso estiver habilitado, você poderá criar políticas de backup que permitem automatizar o gerenciamento simultâneo de várias contas.

Como habilitar o gerenciamento entre contas

1. Abra o Console do AWS Backup em https://console.aws.amazon.com/backup/. Faça login usando as credenciais da sua conta de gerenciamento.
2. No painel de navegação esquerdo, escolha Configurações para abrir a página de gerenciamento entre contas.
3. Na seção Políticas de backup, escolha Habilitar.

   Isso fornece acesso a todas as contas e permite que você crie políticas que automatizam o gerenciamento entre contas em sua organização simultaneamente.
4. Na seção Monitoramento entre contas, escolha Habilitar.

   Isso permite que você monitore as atividades de backup, cópia e restauração de todas as contas em sua organização pela conta de gerenciamento.

Administrador delegado

A administração delegada fornece uma maneira conveniente para os usuários atribuídos em uma conta de membro registrado realizarem a maioria das tarefas AWS Backup administrativas. Você pode optar por delegar a administração de AWS Backup uma conta de membro em AWS Organizations, ampliando assim a capacidade AWS Backup de gerenciar de fora da conta de gerenciamento e em toda a organização.

Uma conta de gerenciamento, por padrão, é a conta usada para editar e gerenciar políticas. Usando o recurso de administrador delegado, é possível delegar essas funções de gerenciamento às contas-membro que você designar. Por sua vez, essas contas poderão gerenciar políticas, além da conta de gerenciamento.

Depois que uma conta-membro for registrada com êxito para administração delegada, ela será uma conta de administrador delegado. Observe que as contas, e não os usuários, são designadas como administradores delegados.

A habilitação de contas de administrador delegado permite a opção de gerenciar políticas de backup, minimiza o número de usuários com acesso à conta de gerenciamento e permite o monitoramento de trabalhos entre contas.

Abaixo está uma tabela mostrando as funções da conta de gerenciamento, contas delegadas como administradores de Backup e contas que são membros da AWS Organização.

> **Note**
>
> As contas de administrador delegado são contas de membro com recursos aprimorados e não podem substituir as configurações de inclusão de serviço de outras contas de membro como uma conta de gerenciamento.

PRIVILÉGIOS	CONTA DE GERENCIAMENTO	ADMINISTRADOR DELEGADO	CONTA-MEMBRO
Registrar/cancelar o registro de contas de administrador delegado	Sim	Não	Não

PRIVILÉGIOS	CONTA DE GERENCIAMENTO	ADMINISTRADOR DELEGADO	CONTA-MEMBRO
Gerencie políticas de backup em todas as contas em AWS Organizations	Sim	Sim	Não
Monitorar trabalhos em várias contas	Sim	Sim	Não

Pré-requisitos

Antes de delegar a administração de backup, você deve primeiro registrar pelo menos uma conta membro em sua AWS organização como administrador delegado. Antes de registrar uma conta como administrador delegado, primeiramente é necessário configurar o seguinte:

- AWS Organizations deve estar habilitado e configurado com pelo menos uma conta de membro, além da sua conta de gerenciamento padrão.
- No AWS Backup console, certifique-se de que as políticas de backup, o monitoramento entre contas e os recursos de backup entre contas estejam ativados. Eles estão abaixo do painel Administradores delegados no console. AWS Backup
  - O monitoramento entre contas permite que você monitore a atividade de backup em todas as contas da sua organização pela conta de gerenciamento, bem como pelas contas de administrador delegado.
  - Opcional: backup entre contas, que permite que as contas da sua organização copiem backups para outras contas (para recursos entre contas compatíveis com backup).
  - Habilite o acesso ao serviço com AWS Backup.

Há duas etapas envolvidas na configuração da administração delegada. A primeira etapa é delegar o monitoramento de trabalhos entre contas. A segunda etapa é delegar o gerenciamento de políticas de backup.

Registrar uma conta-membro como uma conta de administrador delegado

Esta é a primeira seção: Usar o AWS Backup console para registrar uma conta de administrador delegado para monitorar trabalhos entre contas. Para delegar AWS Backup políticas, você usará o console Organizations na próxima seção.

Para registrar uma conta de membro usando o AWS Backup Console:

1. Abra o Console do AWS Backup em https://console.aws.amazon.com/backup/. Faça login usando as credenciais da sua conta de gerenciamento.
2. Em Minha conta, na navegação à esquerda do console, escolha Configurações.
3. No painel Administrador delegado, clique em Registrar administrador delegado ou Adicionar administrador delegado.
4. Na página Registrar administrador delegado, selecione a conta que você deseja registrar e escolha Registrar conta.

Essa conta designada agora será registrada como administrador delegado, com privilégios administrativos para monitorar trabalhos em todas as contas da organização e poderá visualizar e editar políticas (delegação de políticas). Essa conta-membro não poderá registrar ou cancelar o registro de outras contas de administrador delegado. É possível usar o console para registrar até cinco contas como administradores delegados.

Como registrar uma conta-membro de forma programática:

Use o comando de CLI de `register-delegated-administrator`. É possível especificar os seguintes parâmetros em sua solicitação da CLI:

- `service-principal`
- `account-id`

Veja abaixo um exemplo de uma solicitação da CLI para registrar uma conta-membro de forma programática:

```
aws organizations register-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Cancelar o registro de uma conta-membro

Use o procedimento a seguir para remover o acesso administrativo AWS Backup cancelando o registro de uma conta membro em sua AWS organização que já havia sido designada como administrador delegado.

Como cancelar o registro de uma conta-membro usando o console

1. Abra o Console do AWS Backup em https://console.aws.amazon.com/backup/. Faça login usando as credenciais da sua conta de gerenciamento.
2. Em Minha conta, na navegação à esquerda do console, escolha Configurações.
3. Na seção Administrador delegado, clique em Cancelar o registro da conta.
4. Selecione as contas para as quais você deseja cancelar o registro.
5. Na caixa de diálogo Cancelar o registro da conta, analise as implicações de segurança e digite `confirm` para concluir o cancelamento do registro.
6. Selecione `Deregister account`.

Como cancelar o registro de uma conta-membro de forma programática:

Use o comando da CLI `deregister-delegated-administrator` para cancelar o registro de uma conta de administrador delegado. É possível especificar os seguintes parâmetros em sua solicitação de API:

- `service-principal`
- `account-id`

Veja abaixo um exemplo de solicitação da CLI para cancelar o registro programático de uma conta-membro:

```
aws organizations deregister-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Delegar AWS Backup políticas por meio de AWS Organizations

No AWS Organizations console, você pode delegar a administração de várias políticas, incluindo políticas de Backup.

Na conta de gerenciamento conectada ao console do AWS Organizations, é possível criar, visualizar ou excluir uma política de delegação baseada em recursos para sua organização. Para ver as etapas para delegar políticas, consulte Criar uma política de delegação baseada em recursos no Guia do usuário do AWS Organizations .

Como criar uma política de backup

Depois de habilitar o gerenciamento entre contas, crie uma política de backup entre contas a partir da sua conta de gerenciamento.

> **Warning**
>
> Quando você cria uma política com JSON, nomes de chave duplicados serão rejeitados. O nome de cada chave deve ser exclusivo se vários planos, regras ou seleções forem incluídos em uma única política.

Crie uma política de backup por meio do AWS Backup console

1. No painel de navegação à esquerda, escolha Políticas. Na página Políticas de backup, escolha Criar políticas de backup.
2. Na seção Detalhes insira um nome de política de backup e forneça uma descrição.
3. Na seção Detalhes dos planos de backup escolha a guia do editor visual e faça o seguinte:
   a. Em Nome do plano de backup, insira um nome.
   b. Em Regiões, escolha uma região na lista.
4. Na seção Configuração da regra de backup, escolha Adicionar regra de backup.

   O número máximo de regras por plano de backup é 10. Se um plano contiver mais de 10 regras, o plano de backup será ignorado e nenhum backup será criado a partir dele.

   a. Em Nome da regra, insira um nome para a regra. O nome da regra diferencia maiúsculas e minúsculas e pode conter apenas caracteres alfanuméricos ou hífens.
   b. Em Programação, escolha uma frequência de backup na lista Frequência e escolha uma das opções da Janela de backup. Recomendamos que você escolha Usar padrões de janela de backup – recomendado.
5. Em Ciclo de vida, escolha as configurações de ciclo de vida desejadas.

6. Em Nome do cofre de backup, insira um nome. Este é o cofre de backup em que os pontos de recuperação criados por seus backups serão armazenados.

   Certifique-se de que o cofre de backup exista em todas as suas contas. AWS Backup não verifica isso.

7. (opcional) Escolha uma região de destino na lista se quiser que seus backups sejam copiados para outra Região da AWS e adicione tags. É possível escolher tags para os pontos de recuperação criados, independentemente das configurações de cópia entre regiões. Também é possível adicionar mais regras.

8. Na seção Atribuição de recursos, forneça o nome da função AWS Identity and Access Management (IAM). Para usar a função AWS Backup de serviço, forneça`service-role/AWSBackupDefaultServiceRole`.

   AWS Backup assume essa função em cada conta para obter as permissões para realizar trabalhos de backup e cópia, incluindo permissões de chave de criptografia, quando aplicável. AWS Backup também usa essa função para realizar exclusões do ciclo de vida.

   > **Note**
   >
   > AWS Backup não valida se a função existe ou se a função pode ser assumida.
   > Para planos de backup criados pelo gerenciamento de várias contas, AWS Backup usará as configurações opcionais da conta de gerenciamento e substituirá as configurações específicas das contas.
   > Para cada conta à qual você deseja adicionar políticas de backup, é necessário criar os cofres e os perfis do IAM por conta própria.

9. Adicione tags para selecionar os recursos dos quais você deseja fazer backup. O número máximo de tags permitido é 30.

   AWS Organizations A política permite especificar um máximo de 30 tags se um plano de backup for criado por meio da política de Organizations. Tags adicionais podem ser incluídas utilizando várias atribuições de recursos ou envolvendo vários planos de backup.

   Se o número de tags exceder 30 na mesma seleção de backup, seja por meio da modificação da seleção existente ou do uso`@@append`, o plano de backup se tornará inválido e será removido da conta local.

10. Na seção Configurações avançadas, escolha VSS do Windows se o recurso do qual você está fazendo backup estiver executando o Microsoft Windows em uma instância do Amazon EC2. Isso permite que você faça backups do VSS do Windows consistentes com as aplicações.

    > **Note**
    >
    > AWS Backup atualmente oferece suporte a backups consistentes com aplicativos de recursos executados somente no Amazon EC2. Não há compatibilidade com todos os tipos de instância ou de aplicações para backups do VSS do Windows. Para ter mais informações, consulte Criar backups do VSS do Windows.

11. Escolha Adicionar plano de backup para adicioná-lo à política e escolha Criar política de backup.

    A criação de uma política de backup não protege seus recursos até que a política seja anexada às contas. É possível escolher o nome da política e ver os detalhes.

    Veja a seguir um exemplo AWS Organizations de política que cria um plano de backup. Se habilitar o backup do VSS do Windows, você deverá adicionar permissões que permitam fazer backups consistentes com a aplicação, conforme mostrado na seção `advanced_backup_settings` da 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. Na seção Destinos escolha a unidade organizacional ou a conta à qual deseja anexar a política e escolha Anexar. A política também pode ser adicionada a unidades organizacionais ou contas individuais.

> **Note**
>
> Você deve validar a política e certificar-se de incluir todos os campos obrigatórios nela. Se partes da política não forem válidas, o AWS Backup vai ignorar essas partes, mas as partes válidas da política funcionarão conforme o esperado. Atualmente, AWS Backup não valida AWS Organizations as políticas quanto à exatidão.
> Se você aplicar uma política à conta de gerenciamento e uma política diferente a uma conta-membro e elas entrarem em conflito (por exemplo, períodos de retenção de backup diferentes), ambas as políticas serão executadas sem problemas (ou seja, as políticas serão executadas de forma independente para cada conta). Por exemplo, se a política da conta de gerenciamento fizer backup de um volume do Amazon EBS uma

vez por dia e a política local fizer backup de um volume do EBS uma vez por semana, ambas as políticas serão executadas.
Se os campos obrigatórios estiverem ausentes na política efetiva que será aplicada a uma conta (provavelmente devido à mesclagem de diferentes políticas), o AWS Backup não aplicará a política à conta. Se algumas configurações não forem válidas, AWS Backup ajuste-as.

Independentemente das configurações de aceitação em uma conta de membro em um plano de backup criado a partir de uma política de backup, AWS Backup usaremos as configurações de aceitação especificadas na conta de gerenciamento da organização.

Quando você anexar uma diretiva a uma unidade organizacional, cada conta que ingressar nessa unidade organizacional obterá essa política automaticamente e cada conta que é removida da unidade organizacional perderá essa política. Os planos de backup correspondentes são excluídos automaticamente dessa conta.

Monitorar atividades em várias Contas da AWS

Para monitorar trabalhos de backup, cópia e restauração entre contas, é necessário habilitar o monitoramento entre contas. Isso permite que você monitore as atividades de backup em todas as contas da conta de gerenciamento da organização. Depois da inclusão, todos os trabalhos em toda a organização que foram criados após a inclusão ficarão visíveis. Quando você cancela a inclusão, o AWS Backup mantém os trabalhos na exibição agregada por 30 dias (depois de atingir um estado terminal). Os trabalhos criados após o cancelamento da inclusão não ficarão visíveis e nenhum trabalho de backup recém-criado será exibido. Para obter instruções de inclusão, consulte Habilitar o gerenciamento entre contas.

Como monitorar várias contas

1. Abra o Console do AWS Backup em https://console.aws.amazon.com/backup/. Faça login usando as credenciais da sua conta de gerenciamento.
2. No painel de navegação esquerdo, escolha Configurações para abrir a página de gerenciamento entre contas.
3. Na seção Monitoramento entre contas, escolha Habilitar.

Isso permite que você monitore as atividades de backup e restauração de todas as contas em sua organização pela conta de gerenciamento.

4. No painel de navegação à esquerda, escolha Monitoramento entre contas.
5. Na página Monitoramento entre contas, escolha a guia Trabalhos de backup, Trabalhos de restauração ou Trabalhos de cópia para ver todos os trabalhos criados em todas as suas contas. Você pode ver cada um desses trabalhos por Conta da AWS ID e pode ver todos os trabalhos em uma conta específica.
6. Na caixa de pesquisa, filtre os trabalhos por ID da conta, Status ou ID do trabalho.

   Por exemplo, escolha a guia Trabalhos de backup e veja todos os trabalhos de backup criados em todas as suas contas. Filtre a lista por ID da conta e veja todos os trabalhos de backup criados nessa conta.

Regras de inclusão de recursos

Se o plano de backup de uma conta de membro foi criado por uma política de backup em nível de organização, as configurações de AWS Backup aceitação da conta de gerenciamento de organizações substituirão as configurações de aceitação nessa conta de membro, mas somente para esse plano de backup.

Se a conta do membro também tiver planos de backup em nível local criados pelos usuários, esses planos de backup seguirão as configurações de inclusão na conta-membro, sem referência às configurações de inclusão da conta de gerenciamento do Organizations.

Definir políticas, sintaxe de políticas e herança de políticas

Os tópicos a seguir estão documentados no Guia AWS Organizations do usuário.

- Políticas de backup: consulte Políticas de backup.
- Sintaxe da política: consulte Sintaxe e exemplos de política de backup.
- Herança para tipos de políticas de gerenciamento: consulte Herança para tipos de políticas de gerenciamento.

AWS Backup e AWS CloudFormation

No geral

Com o AWS CloudFormation, é possível provisionar e gerenciar seus recursos da AWS de forma segura e repetível usando modelos que você cria. É possível usar modelos do AWS CloudFormation e StackSets para gerenciar seus planos de backup, seleções de recursos de backup e cofres de backup. Para obter informações sobre como usar o AWS CloudFormation, consulte Como o AWS CloudFormation funciona? no Guia do usuário do AWS CloudFormation.

Antes de criar seu modelo ou StackSet do AWS CloudFormation, considere o seguinte:

- Crie modelos separados para seus planos de backup e seus cofres de backup. Só é possível excluir cofres de backup que estejam vazios. Não é possível excluir uma pilha que inclua cofres de backup se elas contiverem pontos de recuperação.
- Antes de criar a pilha, verifique se você tem um perfil de serviço disponível. O perfil de serviço padrão do AWS Backup é criada para você na primeira vez que atribuir recursos a um plano de backup. Se você não atribuiu recursos ao seu plano de backup, faça isso antes de criar a pilha. Você também pode especificar uma função personalizada que criar. Para obter mais informações sobre funções, consulte Perfis de serviço do IAM.

Implantar um cofre de backup, plano de backup e atribuir recursos usando o AWS CloudFormation

Para ver exemplos de modelos AWS CloudFormation que implantam um cofre de backup, planos de backup e a atribuição de recursos, consulte. Atribuindo recursos usando AWS CloudFormation

Implantar planos de backup usando o AWS CloudFormation

Para ver exemplos de AWS CloudFormation modelos que implantam planos de backup, consulte Modelos do AWS CloudFormation para planos de backup.

Implantar frameworks do AWS Backup Audit Manager e planos de relatórios usando o AWS CloudFormation

Para ver exemplos de modelos do AWS CloudFormation que implantam frameworks do AWS Backup Audit Manager e planos de relatórios, consulte Modelos do AWS CloudFormation para planos de backup.

Implantar planos de backup em todas as contas usando o AWS CloudFormation

É possível usar StackSets do AWS CloudFormation em várias contas em um AWS Organization. Modelos de exemplo estão disponíveis no Guia do usuário do AWS CloudFormation.

Um excelente ponto de partida e referência é a publicação Automatizar o backup centralizado em escala em todos os serviços da AWS usando o AWS Backup. Com Ibukun Oyewumi e Sabith Venkitachalapathy (julho de 2021).

Saiba mais sobre o AWS CloudFormation

Para obter informações sobre como usar o AWS CloudFormation com o AWS Backup, consulte Referência de tipo de recurso do AWS Backup no Guia do usuário do AWS CloudFormation.

Para obter informações sobre como controlar o acesso a recursos de serviço da AWS ao usar o AWS CloudFormation, consulte Controle de acesso com o AWS Identity and Access Management no Guia do usuário do AWS CloudFormation.

Segurança em AWS Backup

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS Backup, consulte AWS Serviços no escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade para o AWS Backup inclui, mas não está limitada ao seguinte. Você também é responsável por outros fatores, inclusive a confidencialidade dos dados, os requisitos da organização, as leis e as regulamentações vigentes.
  - Respondendo às comunicações que você recebe AWS.
  - Gerenciar as credenciais que você e sua equipe usam. Para obter mais informações, consulte Gerenciamento de identidade e acesso em AWS Backup.
  - Configurar os planos de backup e as atribuições de recursos para refletir as políticas de proteção de dados da organização. Para obter mais informações, consulte Gerenciar planos de backup.
  - Testar regularmente sua capacidade de encontrar determinados pontos de recuperação e restaurá-los. Para ter mais informações, consulte Trabalhar com backups.
  - Incorporar AWS Backup procedimentos nos procedimentos escritos de recuperação de desastres e continuidade de negócios de sua organização. Para obter um ponto de partida, consulte Introdução ao AWS Backup.
  - Garantir que seus funcionários estejam familiarizados e tenham praticado o uso AWS Backup junto com seus procedimentos organizacionais em caso de emergência. Para obter mais informações, consulte o AWS Well-Architected Framework.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Backup. Os tópicos a seguir mostram como configurar para atender

AWS Backup aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS Backup recursos.

Tópicos

Validação de conformidade para AWS Backup

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA em Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte Referência dos Serviços Qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços com suporte e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Proteção de dados em AWS Backup

AWS Backup está em conformidade com o modelo de responsabilidade AWS compartilhada, que inclui regulamentos e diretrizes para proteção de dados. AWS é responsável por proteger a infraestrutura global que executa todos os AWS serviços. AWS mantém o controle sobre os dados hospedados nessa infraestrutura, incluindo os controles de configuração de segurança para lidar

com o conteúdo do cliente e os dados pessoais. AWS clientes e AWS parceiros da Partner Network (APN), atuando como controladores ou processadores de dados, são responsáveis por quaisquer dados pessoais que coloquem no. Nuvem AWS

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure contas de usuário individuais com AWS Identity and Access Management (IAM). Isto ajuda a garantir que cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use o Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para se comunicar com os recursos da AWS .
- Use soluções AWS de criptografia, juntamente com todos os controles de segurança padrão nos AWS serviços.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de conta dos seus clientes, em campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS Backup ou outros AWS serviços usando o console, a API ou AWS os SDKs. AWS CLI Todos os dados inseridos por você no AWS Backup ou em outros serviços podem ser separados para inclusão em logs de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar a solicitação a esse servidor.

Para mais informações sobre proteção de dados, consulte a publicação Modelo de responsabilidade compartilhada da AWS e do GDPR no Blog de segurança da AWS .

Criptografia para backups em AWS Backup

> **Note**
>
> AWS Backup O Audit Manager ajuda você a detectar automaticamente backups não criptografados.

Você pode configurar a criptografia para tipos de recursos que oferecem suporte ao AWS Backup gerenciamento total do uso AWS Backup. Se o tipo de recurso não oferecer suporte ao AWS Backup gerenciamento completo, você deverá configurar sua criptografia de backup seguindo as instruções

desse serviço, como a criptografia do Amazon EBS no Guia do Usuário do Amazon Elastic Compute Cloud. Para ver a lista de tipos de recursos que oferecem suporte ao AWS Backup gerenciamento completo, consulte a seção “ AWS Backup Gerenciamento completo” da Disponibilidade de recursos por recurso tabela.

A tabela a seguir lista cada tipo de recurso com suporte, como a criptografia é configurada para backups e se a criptografia independente para backups é compatível. Quando o AWS Backup criptografa um backup de forma independente, ele usa o algoritmo de criptografia AES-256 padrão do setor.

Tipo de recurso	Como configurar a criptografia	AWS Backup Criptografia independente
Amazon Simple Storage Service (Amazon S3)	Os backups do Amazon S3 são criptografados usando uma chave AWS KMS (AWS Key Management Service) associada ao cofre de backup. A chave AWS KMS pode ser uma CMK gerenciada pelo cliente ou uma CMK AWS gerenciada associada ao serviço. AWS Backup AWS Backup criptografa todos os backups, mesmo que os buckets de origem do Amazon S3 não estejam criptogra fados.	Compatível
Máquinas virtuais da VMware	Os backups da VM são sempre criptografados. A chave de AWS KMS criptogra fia para backups de máquinas virtuais é configurada no AWS Backup cofre no qual os backups da máquina virtual são armazenados.	Compatível

Tipo de recurso	Como configurar a criptografia	AWS Backup Criptografia independente
Amazon DynamoDB após a habilitar Backup avançado do DynamoDB	Os backups do DynamoDB sempre são criptografados. A chave AWS KMS de criptografia para backups do DynamoDB é configurada no cofre em que os backups AWS Backup do DynamoDB são armazenados.	Compatível

Tipo de recurso	Como configurar a criptografia	AWS Backup Criptografia independente
Amazon DynamoDB sem habilitar Backup avançado do DynamoDB	Os backups do DynamoDB são criptografados automatic amente com a mesma chave de criptografia que foi usada para criptografar a tabela de origem do DynamoDB. Os snapshots das tabelas não criptografadas do DynamoDB também não são criptogra fados. **Note** AWS Backup Para criar um backup de uma tabela criptogra fada do DynamoDB, você deve adicionar `kms:Decrypt` as permissõe s `kms:Gener ateDataKey` e a função do IAM usada para backup. Como alternativa, você pode usar a função de serviço AWS Backup padrão.	Não suportado

Tipo de recurso	Como configurar a criptografia	AWS Backup Criptografia independente
Amazon Elastic File System (Amazon EFS)	Os backups do Amazon EFS sempre são criptografados. A chave de AWS KMS criptografia para backups do Amazon EFS é configurada no AWS Backup cofre em que os backups do Amazon EFS são armazenados.	Compatível
Amazon Elastic Block Store (Amazon EBS)	Por padrão, os backups do Amazon EBS são criptografados usando a chave usada para criptografar o volume de origem ou não são criptografados. Durante a restauração, é possível optar por substituir o método de criptografia padrão especificando uma chave do KMS.	Não suportado
AMIs do Amazon Elastic Compute Cloud (Amazon EC2)	As AMIs não são criptografadas. Os snapshots do EBS são criptografados pelas regras de criptografia padrão para backups do EBS (consulte a entrada do EBS). Os instantâneos de dados e volumes raiz do EBS podem ser criptografados e anexados a uma AMI.	Não suportado

Tipo de recurso	Como configurar a criptografia	AWS Backup Criptografia independente
Amazon Relational Database Service (Amazon RDS)	Os snapshots do Amazon RDS são criptografados automaticamente com a mesma chave de criptografia que foi usada para criptografar banco de dados de origem do Amazon RDS. Os snapshots de bancos de dados do Amazon RDS não criptografados também não são criptografados. **Note** AWS Backup atualmente oferece suporte a todos os mecanismos de banco de dados do Amazon RDS, incluindo o Amazon Aurora.	Não suportado
Amazon Aurora	Os snapshots do cluster do Aurora são criptografados automaticamente com a mesma chave de criptografia que foi usada para criptografar o cluster de origem do Amazon Aurora. Os snapshots de clusters não criptografados do Aurora também não são criptografados.	Não suportado

Tipo de recurso	Como configurar a criptografia	AWS Backup Criptografia independente
AWS Storage Gateway	Os snapshots do Storage Gateway são criptografados automaticamente com a mesma chave de criptografia que foi usada para criptografar o volume de origem do Storage Gateway. Os snapshots de volumes não criptografados do Storage Gateway também não são criptografados. **Note** Não é necessário usar uma chave gerenciada pelo cliente em todos os serviços para habilitar o Storage Gateway. Só é necessário copiar o backup do Storage Gateway em um cofre que configurou uma chave do KMS. Isso ocorre porque o Storage Gateway não tem uma chave AWS KMS gerenciada específica do serviço.	Não suportado

Tipo de recurso	Como configurar a criptografia	AWS Backup Criptografia independente
Amazon FSx	Os recursos de criptografia para os sistemas de arquivos do Amazon FSx diferem com base no sistema de arquivos subjacente. Para saber mais sobre seu sistema de arquivos Amazon FSx específico, consulte o Guia do usuário do FSx apropriado.	Não suportado
Amazon DocumentDB	Os snapshots do cluster do Amazon DocumentDB são criptografados automatic amente com a mesma chave de criptografia que foi usada para criptografar o cluster de origem do Amazon DocumentDB. Os snapshots de clusters não criptografados do Amazon DocumentDB também não são criptogra fados.	Não suportado
Amazon Neptune	Os snapshots do cluster do Neptune são criptografados automaticamente com a mesma chave de criptografia que foi usada para criptogra far o cluster de origem do Neptune. Os snapshots de clusters não criptografados do Neptune também não são criptografados.	Não suportado

Tipo de recurso	Como configurar a criptografia	AWS Backup Criptografia independente
Amazon Timestream	Os backups de snapshots de tabelas do Timestream são sempre criptografados. A chave de criptografia do AWS KMS para backups do Timestream é configurada no cofre de backup no qual os backups do Timestream são armazenados.	Compatível
Amazon Redshift	Os snapshots do cluster do Amazon Redshift são criptografados automatic amente com a mesma chave de criptografia que foi usada para criptografar o cluster de origem do Amazon Redshift. Os snapshots de clusters não criptografados do Amazon Redshift também não são criptografados.	Não suportado
AWS CloudFormation	CloudFormation os backups são sempre criptografados. A chave de CloudFormation criptografia para CloudForm ation backups é configura da no CloudFormation cofre no qual os CloudFormation backups são armazenados.	Compatível

Tipo de recurso	Como configurar a criptografia	AWS Backup Criptografia independente
Backup de bancos de dados SAP HANA em instâncias do Amazon EC2	Os backups do banco de dados SAP HANA são sempre criptografados. A chave de AWS KMS criptografia para backups do banco de dados do SAP HANA é configura da no AWS Backup cofre no qual os backups do banco de dados são armazenados.	Compatível

Criptografia para cópias de backup

Quando você usa AWS Backup para copiar seus backups em contas ou regiões, criptografa AWS Backup automaticamente essas cópias para a maioria dos tipos de recursos, mesmo que o backup original não esteja criptografado. AWS Backup criptografa sua cópia usando a chave KMS do cofre de destino. No entanto, os snapshots dos clusters não criptografados do Aurora, do Amazon DocumentDB e do Neptune também não são criptografados.

Criptografia e cópias de backup

A cópia entre contas com chaves KMS AWS gerenciadas não é compatível com recursos que não são totalmente gerenciados pelo. AWS Backup Consulte AWS Backup Gerenciamento completo para determinar quais recursos são totalmente gerenciados.

Para os recursos totalmente gerenciados pelo AWS Backup, os backups são criptografados com a chave de criptografia do cofre de backup. Para os recursos que não são totalmente gerenciados pelo AWS Backup, as cópias entre contas usam a mesma chave KMS do recurso de origem. Para mais informações, consulte Chaves de criptografia e cópias entre contas.

Criptografia de credenciais de hipervisor de máquina virtual

As máquinas virtuais gerenciadas por um hipervisor usam o AWS Backup Gateway para conectar sistemas on-premises ao AWS Backup. É importante que os hipervisores tenham a mesma segurança robusta e confiável. Essa segurança pode ser obtida criptografando o hipervisor, seja por chaves AWS próprias ou por chaves gerenciadas pelo cliente.

AWS chaves próprias e gerenciadas pelo cliente

AWS Backup fornece criptografia para as credenciais do hipervisor para proteger as informações confidenciais de login do cliente usando chaves de criptografia AWS próprias. Em vez disso, você tem a opção de usar chaves gerenciadas pelo cliente.

Por padrão, as chaves usadas para criptografar as credenciais em seu hipervisor são AWS chaves próprias. AWS Backup usa essas chaves para criptografar automaticamente as credenciais do hipervisor. Você não pode visualizar, gerenciar ou usar chaves AWS próprias, nem auditar seu uso. No entanto, não é necessário tomar nenhuma medida nem alterar qualquer programa para proteger as chaves que criptografam seus dados. Para obter mais informações, consulte chaves AWS próprias no Guia do AWS KMS desenvolvedor.

Como alternativa, as credenciais podem ser criptografadas usando chaves gerenciadas pelo cliente. O AWS Backup é compatível com o uso de chaves simétricas gerenciadas pelo cliente que você cria, tem a propriedade e gerencia para executar a criptografia. Como você tem controle total dessa criptografia, é possível realizar tarefas como:

- Estabelecer e manter as políticas de chave
- Estabelecer e manter subsídios e políticas do IAM
- Habilitar e desabilitar políticas de chaves
- Alternar os materiais de criptografia de chaves
- Adicionar etiquetas
- Criar aliases de chaves
- Chaves de agendamento para exclusão

Ao usar uma chave gerenciada pelo cliente, AWS Backup valida se sua função tem permissão para descriptografar usando essa chave (antes da execução de um trabalho de backup ou restauração). Você deve adicionar a ação `kms:Decrypt` à função usada para iniciar um trabalho de backup ou de restauração.

Como não é possível adicionar a ação `kms:Decrypt` à função de backup padrão, você deve usar uma função diferente da função de backup padrão para usar as chaves gerenciadas pelo cliente.

Para obter mais informações, consulte chaves gerenciadas pelo cliente no Guia do desenvolvedor do AWS Key Management Service .

Concessão necessária ao usar chaves gerenciadas pelo cliente

AWS KMS exige uma concessão para usar sua chave gerenciada pelo cliente. Quando você importa uma configuração de hipervisor criptografada com uma chave gerenciada pelo cliente, AWS Backup cria uma concessão em seu nome enviando uma `CreateGrant`solicitação para AWS KMS. AWS Backup usa concessões para acessar uma chave KMS em uma conta de cliente.

Você pode revogar o acesso à concessão ou remover AWS Backup o acesso à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, todos os seus gateways associados ao seu hipervisor não poderão mais acessar o nome de usuário e a senha do hipervisor criptografados pela chave gerenciada pelo cliente, o que afetará os trabalhos de backup e de restauração. Especificamente, haverá falha nos trabalhos de backup e de restauração que você executa nas máquinas virtuais desse hipervisor.

O gateway de backup usa a operação `RetireGrant` para remover uma concessão quando você exclui um hipervisor.

Monitorar as chaves de criptografia

Ao usar uma chave gerenciada pelo AWS KMS cliente com seus AWS Backup recursos, você pode usar AWS CloudTrailo Amazon CloudWatch Logs para rastrear solicitações AWS Backup enviadas para AWS KMS.

Procure AWS CloudTrail eventos com os seguintes `"eventName"` campos para monitorar AWS KMS as operações chamadas por AWS Backup para acessar dados criptografados pela chave gerenciada pelo cliente:

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`
- `"eventName": "DescribeKey"`

Gerenciamento de identidade e acesso em AWS Backup

O acesso a AWS Backup requer credenciais. Essas credenciais devem ter permissões para acessar os recursos da AWS , como um banco de dados do Amazon DynamoDB ou um sistema de arquivos do Amazon EFS. Além disso, os pontos de recuperação criados AWS Backup por alguns serviços

AWS Backup suportados não podem ser excluídos usando o serviço de origem (como o Amazon EFS). Você pode excluir esses pontos de recuperação usando AWS Backup.

As seções a seguir fornecem detalhes sobre como você pode usar o AWS Identity and Access Management (IAM) e como ajudar AWS Backup a proteger o acesso aos seus recursos.

> **Warning**
>
> AWS Backup usa a mesma função do IAM que você escolheu ao atribuir recursos para gerenciar o ciclo de vida do seu ponto de recuperação. Se você excluir ou modificar essa função, AWS Backup não poderá gerenciar o ciclo de vida do ponto de recuperação. Quando isso ocorrer, ele tentará usar uma função vinculada ao serviço para gerenciar o ciclo de vida. Em uma pequena porcentagem dos casos, isso também pode não funcionar, deixando pontos de recuperação `EXPIRED` em seu armazenamento, o que pode gerar custos indesejados. Para excluir pontos de recuperação `EXPIRED`, exclua-os manualmente usando o procedimento em Excluir backups.

Tópicos

Autenticação

O acesso AWS Backup ou os AWS serviços dos quais você está fazendo backup exigem credenciais que AWS possam ser usadas para autenticar suas solicitações. Você pode acessar AWS como qualquer um dos seguintes tipos de identidades:

- Conta da AWS usuário root — Ao se inscrever AWS, você fornece um endereço de e-mail e uma senha associados à sua AWS conta. Esse será seu usuário raiz da Conta da AWS . Suas credenciais fornecem acesso completo a todos os seus AWS recursos.

> **Important**
>
> Por motivos de segurança, recomendamos usar o usuário raiz apenas para criar um administrador. O administrador é um usuário do IAM com permissões totais para sua Conta da AWS. Você então poderá usar esse usuário administrador para criar outros usuários e perfis do IAM com permissões limitadas. Para obter mais informações, consulte Práticas recomendadas do IAM e Criação do seu primeiro usuário administrador e grupo do IAM no Manual do usuário do IAM.

- Usuário do IAM: um usuário do IAM é uma identidade em sua Conta da AWS com permissões personalizadas específicas (por exemplo, permissões para criar um cofre de backup no qual seus backups serão armazenados). Você pode usar um nome de usuário e uma senha do IAM para entrar em AWS páginas da Web seguras AWS Management Console, como os Fóruns de AWS discussão ou o AWS Support Centro.

  Além do nome de usuário e senha, você também pode gerar chaves de acesso para cada usuário. Você pode usar essas chaves ao acessar AWS serviços programaticamente, por meio de um dos vários SDKs ou usando a (AWS Command Line Interface CLI AWS). As ferramentas de SDK e de AWS CLI usam as chaves de acesso para o cadastramento criptográfico da sua solicitação. Se você não utilizar ferramentas da AWS , cadastre a solicitação você mesmo. Para obter mais informações sobre a autenticação de solicitações, consulte Processo de cadastramento do Signature versão 4 na Referência geral da AWS.
- Perfil do IAM: um perfil do IAM é uma identidade do IAM que você pode criar em sua conta com permissões específicas. É semelhante a um usuário do IAM, mas não está associada a uma pessoa específica. Uma função do IAM permite que você obtenha chaves de acesso temporárias que podem ser usadas para acessar AWS serviços e recursos. Funções do IAM com credenciais temporárias são úteis nas seguintes situações:
  - Acesso de usuário federado — em vez de criar um usuário do IAM, você pode usar identidades de usuário preexistentes do diretório de AWS Directory Service usuários corporativo ou de um provedor de identidade da web. Eles são conhecidos como usuários federados. A AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidades. Para obter mais informações sobre usuários federados, consulte Usuários federados e funções no Manual do usuário do IAM.
  - Administração de várias contas — você pode usar uma função do IAM em sua conta para conceder outras Conta da AWS permissões para administrar os recursos da sua conta. Para ver

um exemplo, consulte Tutorial: Delegar acesso ao Contas da AWS uso de funções do IAM no Guia do usuário do IAM.

- AWS acesso ao serviço — Você pode usar uma função do IAM em sua conta para conceder permissões a um AWS serviço para acessar os recursos da sua conta. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS serviço no Guia do usuário do IAM.
- Aplicativos em execução no Amazon Elastic Compute Cloud (Amazon EC2) — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos executados em uma instância do Amazon EC2 e fazer solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na instância EC2 obtenham credenciais temporárias. Para obter mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicativos em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Controle de acesso

Você pode ter credenciais válidas para autenticar suas solicitações, mas, a menos que tenha as permissões apropriadas, não poderá acessar AWS Backup recursos como cofres de backup. Você também não pode fazer backup de AWS recursos como volumes do Amazon Elastic Block Store (Amazon EBS).

Cada AWS recurso é de propriedade de um Conta da AWS, e as permissões para criar ou acessar um recurso são regidas por políticas de permissões. Um administrador da conta pode anexar políticas de permissões às identidades AWS Identity and Access Management (IAM) (ou seja, usuários, grupos e funções). E alguns serviços também são compatíveis com anexar políticas de permissões aos recursos.

> **Note**
>
> O administrador de uma conta (ou o usuário administrador) é um usuário com permissões de administrador. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Ao conceder permissões, você decide quem recebe as permissões, os recursos relacionados às permissões concedidas e as ações específicas que deseja permitir nesses recursos.

As seções a seguir abordam como políticas de acesso funcionam e como você pode usá-las para proteger seus backups.

Tópicos

Recursos e operações

Um recurso é um objeto que existe dentro de um serviço. AWS Backup os recursos incluem planos de backup, cofres de backup e backups. Backup é um termo geral que se refere aos vários tipos de recursos de backup existentes em AWS. Por exemplo, snapshots do Amazon EBS, snapshots do Amazon Relational Database Service (Amazon RDS) e backups do Amazon DynamoDB são todos os tipos de recursos de backup.

Em AWS Backup, os backups também são chamados de pontos de recuperação. Ao usar AWS Backup, você também trabalha com os recursos de outros AWS serviços que está tentando proteger, como volumes do Amazon EBS ou tabelas do DynamoDB. Esses recursos têm nomes de recurso da Amazon (ARNs) exclusivos associados a eles. Os ARNs identificam recursos de forma exclusiva. AWS É necessário ter um ARN quando você precisar especificar um recurso sem ambiguidade em toda a AWS como, políticas do IAM ou chamadas de API.

A tabela a seguir lista recursos, sub-recursos e formatos de ARN.

AWS Backup ARNs de recursos

Tipo de recurso	Formato ARN	Exemplo de ID exclusivo
Plano de backup	`arn:aws:backup:region:account-id:backup-plan:*`	
Cofre de backup	`arn:aws:backup:region:account-id:backup-vault:*`	
Ponto de recuperação para o Amazon EBS	`arn:aws:ec2:region::snapshot/*`	`snapshot/snap-05f426fd8kdjb4224`
Ponto de recuperação para imagens do Amazon EC2	`arn:aws:ec2:region::image/ami-*`	`image/ami-1a2b3e4f5e6f7g890`
Ponto de recuperação para o Amazon RDS	`arn:aws:rds:region:account-id:snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Ponto de recuperação para o Aurora	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Ponto de recuperação para o Storage Gateway	`arn:aws:ec2:region::snapshot/*`	`snapshot/snap-0d40e49137e31d9e0`
Ponto de recuperação para o DynamoDB sem Backup avançado do DynamoDB	`arn:aws:dynamodb:region:account-id:table/*/backup/*`	`table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3`

Tipo de recurso	Formato ARN	Exemplo de ID exclusivo
Ponto de recuperação para o DynamoDB com Backup avançado do DynamoDB habilitado	`arn:aws:backup:region:account-id:recovery-point:*`	`12a34a56-7bb8-901c-cd23-4567d8e9ef01`
Ponto de recuperação para o Amazon EFS	`arn:aws:backup:region:account-id:recovery-point:*`	`d99699e7-e183-477e-bfcd-ccb1c6e5455e`
Ponto de recuperação para o Amazon FSx	`arn:aws:fsx:region:account-id:backup/backup-*`	`backup/backup-1a20e49137e31d9e0`
Ponto de recuperação para máquina virtual	`arn:aws:backup:region:account-id:recovery-point:*`	`1801234a-5b6b-7dc8-8032-836f7ffc623b`
Ponto de recuperação para backup contínuo do Amazon S3	`arn:aws:backup:region:account-id:recovery-point:*`	`my-bucket -5ec207d0`
Ponto de recuperação para backup periódico do S3	`arn:aws:backup:region:account-id:recovery-point:*`	`my-bucket -20211231900000-5ec207d0`
Ponto de recuperação para Amazon DocumentDB	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Ponto de recuperação para Neptune	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`

Tipo de recurso	Formato ARN	Exemplo de ID exclusivo
Ponto de recuperação para o Amazon Redshift	`arn:aws:redshift:region:account-id:snapshot:resource/awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Ponto de recuperação para Amazon Timestream	`arn:aws:backup:region:account-id:recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta`
Ponto de recuperação para AWS CloudFormation modelo	`arn:aws:backup:region:account-id:recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`
Ponto de recuperação para banco de dados SAP HANA na instância do Amazon EC2	`arn:aws:backup:region:account-id:recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`

Todos os recursos que oferecem suporte ao AWS Backup gerenciamento completo têm pontos de recuperação no formato`arn:aws:backup:region:account-id:recovery-point:*`, facilitando a aplicação de políticas de permissões para proteger esses pontos de recuperação. Para ver quais recursos oferecem suporte ao AWS Backup gerenciamento completo, consulte essa seção da Disponibilidade de recursos por recurso tabela.

AWS Backup fornece um conjunto de operações para trabalhar com AWS Backup recursos. Para ver uma lista das operações disponíveis, consulte AWS Backup Ações.

Propriedade de recursos

Ele Conta da AWS possui os recursos que são criados na conta, independentemente de quem criou os recursos. Especificamente, o proprietário Conta da AWS do recurso é a entidade principal (ou seja, o usuário Conta da AWS raiz, um usuário do IAM ou uma função do IAM) que autentica a solicitação de criação do recurso. Os seguintes exemplos mostram como isso funciona:

- Se você usar suas credenciais de usuário Conta da AWS raiz Conta da AWS para criar um cofre de backup, você Conta da AWS é o proprietário do cofre.
- Se você criar um usuário do IAM em seu Conta da AWS e conceder permissões para criar um cofre de backup para esse usuário, o usuário poderá criar um cofre de backup. No entanto, sua conta da AWS , à qual o usuário pertence, é a proprietária do recurso do cofre de backup.
- Se você criar uma função do IAM na sua Conta da AWS com permissões para criar um cofre de backup, qualquer pessoa que possa assumir a função poderá criar um cofre. Seu Conta da AWS, ao qual a função pertence, é proprietário do recurso de backup vault.

Especificando elementos de política: ações, efeitos e entidades principais

Para cada AWS Backup recurso (consulteRecursos e operações), o serviço define um conjunto de operações de API (consulteAções). Para conceder permissões para essas operações de API, AWS Backup defina um conjunto de ações que você pode especificar em uma política. A execução de uma operação de API pode exigir permissões para mais de uma ação.

Estes são os elementos de política mais básicos:

- Recurso: em uma política, você usa um nome do recurso da Amazon (ARN) para identificar o recurso a que a política se aplica. Para ter mais informações, consulte Recursos e operações.
- Ação: você usa palavras-chave de ação para identificar operações de recursos que deseja permitir ou negar.
- Efeito: você especifica o efeito quando o usuário solicita a ação específica, que pode ser permitir ou negar. Se você não conceder (permitir) explicitamente acesso a um recurso, o acesso estará implicitamente negado. Você também pode negar explicitamente o acesso a um recurso, para ter certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso.
- Entidade principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é a entidade principal implícita. Para as políticas baseadas em recursos, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam permissões (isso se aplica somente a políticas baseadas em recursos).

Para saber mais sobre a sintaxe e as descrições de políticas do IAM, consulte a Referência da política JSON do IAM no Guia do usuário do IAM.

Para ver uma tabela mostrando todas as ações AWS Backup da API, consulte Permissões da API: referência de ações, recursos e condições.

Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem da política do IAM para especificar as condições de quando uma política deverá entrar em vigor. Por exemplo, é recomendável aplicar uma política somente após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política, consulte Condition no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

AWS Backup define seu próprio conjunto de chaves de condição. Para ver uma lista de chaves de AWS Backup condição, consulte Chaves de condição AWS Backup na Referência de autorização de serviço.

Permissões da API: referência de ações, recursos e condições

Ao configurar Controle de acesso e escrever uma política de permissões que você pode anexar a uma identidade do IAM (políticas baseadas em identidade), é possível usar a lista de a seguir como referência. A lista de inclui cada operação de AWS Backup API, as ações correspondentes para as quais você pode conceder permissões para realizar a ação e o AWS recurso para o qual você pode conceder as permissões. Você especifica as ações no campo `Action` da política e o valor do recurso no campo `Resource` da política. Se o campo `Resource` estiver em branco, use o caractere curinga (`*`) para incluir todos os recursos.

Você pode usar chaves AWS de condição abrangentes em suas AWS Backup políticas para expressar condições. Para obter uma lista completa AWS de chaves gerais, consulte Chaves disponíveis no Guia do usuário do IAM.

[1] Usa a política de acesso ao cofre existente.

[2] Consulte os AWS Backup ARNs de recursos ARNs de pontos de recuperação específicos do recurso.

[3] `StartRestoreJob` deve ter o par de valores-chave nos metadados do recurso. Para obter os metadados do recurso, chame a API `GetRecoveryPointRestoreMetadata`.

[4] Certos tipos de recursos exigem que a função que executa o backup tenha uma permissão de marcação específica `backup:TagResource` se você planeja incluir tags de recursos originais em seu backup ou adicionar tags adicionais a um backup. Qualquer backup com um ARN começando com `arn:aws:backup:region:account-id:recovery-point:` ou um backup contínuo requer essa permissão. `backup:TagResource`a permissão deve ser aplicada a `"resourcetype": "arn:aws:backup:region:account-id:recovery-point:*"`

Para obter mais informações, consulte Ações, recursos e chaves de condição do AWS Backup, na Referência de autorização do serviço.

Copiar permissões de tags

Quando AWS Backup executa um trabalho de backup ou cópia, ele tenta copiar as tags do seu recurso de origem (ou ponto de recuperação, no caso de cópia) para o seu ponto de recuperação.

> **Note**
>
> AWS Backup não copia as tags de forma nativa durante os trabalhos de restauração. Para uma arquitetura orientada por eventos que copiará tags durante trabalhos de restauração, consulte Como reter tags de recursos em trabalhos de AWS Backup restauração.

Durante um trabalho de backup ou cópia, AWS Backup agrega as tags que você especifica em seu plano de backup (ou plano de cópia, ou backup sob demanda) com as tags do seu recurso de origem. No entanto, AWS impõe um limite de 50 tags por recurso, que AWS Backup não pode exceder. Quando um trabalho de backup ou de cópia agrega tags do plano e do recurso de origem, ele pode descobrir mais de 50 tags no total. Ele não conseguirá concluir o trabalho e haverá falhar no trabalho. Isso é consistente com as melhores práticas AWS de marcação em todo o mundo. Para saber mais, consulte Limites de tags no Guia de referência geral da AWS .

- Seu recurso tem mais de 50 tags depois de agregar suas tags de trabalho de backup às tags de recursos de origem. AWS suporta até 50 tags por recurso. Para obter mais informações, consulte Limites de tags.
- A função do IAM que você fornece AWS Backup não tem permissões para ler as tags de origem ou definir as tags de destino. Para obter mais informações e exemplos de políticas de perfil do IAM, consulte Políticas gerenciadas.

Você pode usar seu plano de backup para criar tags que contradizem suas tags do recursos de origem. Quando entram em conflito, as tags do plano de backup têm precedência. Use essa técnica se você preferir não copiar um valor de tag do seu recurso de origem. Especifique a mesma chave de tag, mas com um valor diferente ou vazio, usando o plano de backup.

Permissões necessárias para atribuir tags a backups

Tipo de recurso	Permissão obrigatória
Sistema de arquivos do Amazon EFS	`elasticfilesystem:DescribeTags`
Sistema de arquivos do Amazon FSx	`fsx:ListTagsForResource`
Banco de dados do Amazon RDS e cluster do Amazon Aurora	`rds:AddTagsToResource` `rds:ListTagsForResource`
Volume do Storage Gateway	`storagegateway:ListTagsForResource`
Instância do Amazon EC2 e volume do Amazon EBS	`EC2:CreateTags` `EC2:DescribeTags`

O DynamoDB não é compatível com a atribuição de tags aos backups, a menos que você habilite Backup avançado do DynamoDB primeiro.

Quando um backup do Amazon EC2 cria um ponto de recuperação de imagem e um conjunto de snapshots, AWS Backup copia as tags para a AMI resultante. AWS Backup também copia as tags dos volumes associados à instância do Amazon EC2 para os snapshots resultantes.

Políticas de acesso

A política de permissões descreve quem tem acesso a quê. As políticas anexadas a uma identidade do IAM são conhecidas como políticas baseadas em identidade (políticas do IAM). As políticas anexadas a um recurso são chamadas de políticas baseadas em recursos. AWS Backup suporta políticas baseadas em identidade e políticas baseadas em recursos.

> **Note**
>
> Esta seção discute o uso do IAM no contexto de AWS Backup. Não são fornecidas informações detalhadas sobre o serviço IAM. Para obter a documentação completa do IAM, consulte O que é o IAM? no Manual do usuário do IAM. Para obter informações sobre a sintaxe e as descrições da política do IAM, consulte a Referência da política JSON do IAM no Manual do usuário do IAM.

Políticas baseadas em identidade (políticas do IAM)

As políticas baseadas em identidade são políticas que podem ser anexadas a identidades do IAM, como usuários ou funções. Por exemplo, você pode definir uma política que permita que um usuário visualize e faça backup de AWS recursos, mas impeça que ele restaure os backups.

Para obter mais informações sobre usuários, grupos, funções e permissões, consulte Identidades (usuários, grupos e funções) no Guia do usuário do IAM.

Para obter mais informações sobre como usas as políticas do IAM para controlar o acesso a backups, consulte Políticas gerenciadas para AWS Backup.

Políticas baseadas em recursos

AWS Backup oferece suporte a políticas de acesso baseadas em recursos para cofres de backup. Isso permite que você defina uma política de acesso que controle quais usuários têm que tipo de acesso a qualquer um dos backups organizados em um cofre de backup. As políticas de acesso baseadas em recursos para cofres de backup fornecem uma maneira fácil de controlar o acesso aos seus backups.

As políticas de acesso do Backup Vault controlam o acesso do usuário quando você usa AWS Backup APIs. Alguns tipos de backup, como snapshots do Amazon Elastic Block Store (Amazon EBS) e do Amazon Relational Database Service (Amazon RDS), também podem ser acessados usando as APIs desses serviços. É possível criar políticas de acesso separadas no IAM, que controlam o acesso a essas APIs, para controlar totalmente o acesso aos backups.

Para saber como criar uma política de acesso para cofres de backup, consulte Definir políticas de acesso em cofres de backup.

Perfis de serviço do IAM

Uma função AWS Identity and Access Management (IAM) é semelhante à de um usuário, pois é uma AWS identidade com políticas de permissões que determinam o que a identidade pode ou não fazer AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, o propósito do perfil é ser assumido por qualquer pessoa que precisar dele. Uma função de serviço é uma função que um AWS serviço assume para realizar ações em seu nome. Como um serviço que executa as operações de backup em seu nome, o AWS Backup exige que você atribua uma função a ele ao executar operações de backup em seu nome. Para obter mais informações sobre perfis do IAM, consulte Perfis do IAM no Guia do usuário do IAM.

A função para a qual você passa AWS Backup deve ter uma política do IAM com as permissões que permitem AWS Backup realizar ações associadas às operações de backup, como criar, restaurar ou expirar backups. Permissões diferentes são necessárias para cada um dos AWS serviços que oferecem AWS Backup suporte. A função também deve estar AWS Backup listada como uma entidade confiável, o que AWS Backup permite assumir a função.

Ao atribuir recursos a um plano de backup ou realizar um backup, cópia ou restauração sob demanda, você deve transmitir uma função de serviço que tenha acesso para realizar as operações subjacentes nos recursos especificados. AWS Backup usa essa função para criar, marcar e excluir recursos em sua conta.

Usando AWS funções para controlar o acesso aos backups

Você pode usar funções para controlar o acesso aos seus backups definindo funções com escopo limitado e especificando quem pode transmitir essa função ao AWS Backup. Por exemplo, você pode criar uma função que conceda somente permissões para fazer backup dos bancos de dados do Amazon Relational Database Service (Amazon RDS) e conceda somente aos proprietários do banco de dados do Amazon RDS permissão para transmitir essa função para. AWS Backup AWS Backup fornece várias políticas gerenciadas predefinidas para cada um dos serviços suportados. Essas políticas gerenciadas podem ser anexadas a funções criadas por você. Isso facilita a criação de funções específicas do serviço que tenham as permissões corretas necessárias. AWS Backup

Para obter mais informações sobre políticas AWS gerenciadas para AWS Backup, consultePolíticas gerenciadas para AWS Backup.

Função de serviço padrão para AWS Backup

Ao usar o AWS Backup console pela primeira vez, você pode optar por AWS Backup criar uma função de serviço padrão para você. Essa função tem as permissões AWS Backup necessárias para criar e restaurar backups em seu nome.

> **Note**
>
> O perfil padrão é criado automaticamente quando você usa o AWS Management Console. Você pode criar a função padrão usando o AWS Command Line Interface (AWS CLI), mas isso deve ser feito manualmente.

Se preferir usar perfis personalizados, como perfis separados para diferentes tipos de recursos, você também poderá fazer isso e passar os perfis personalizados para o AWS Backup. Para ver exemplos de funções que permitem o backup e a restauração para tipos de recursos individuais, consulte a tabela Políticas gerenciadas pelo cliente.

A função de serviço padrão é nomeada`AWSBackupDefaultServiceRole`. Essa função de serviço contém duas políticas gerenciadas AWSBackupServiceRolePolicyForBackup`AWSBackupServiceRolePolicyForRestores`e.

`AWSBackupServiceRolePolicyForBackup`inclui uma política do IAM que concede AWS Backup permissões para descrever o recurso que está sendo copiado, a capacidade de criar, excluir, descrever ou adicionar tags a um backup, independentemente da AWS KMS chave com a qual ele está criptografado.

`AWSBackupServiceRolePolicyForRestores`inclui uma política do IAM que concede AWS Backup permissões para criar, excluir ou descrever o novo recurso que está sendo criado a partir de um backup, independentemente da AWS KMS chave com a qual ele está criptografado. Ele também inclui permissões para marcar o recurso recém-criado.

Para restaurar uma instância do Amazon EC2, você deve executar uma nova instância.

Criar o perfil de serviço padrão no console

As ações específicas que você executa no AWS Backup console criam a função de serviço AWS Backup padrão.

Para criar a função de serviço AWS Backup padrão em sua AWS conta

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Para criar o perfil para sua conta, atribua recursos a um plano de backup ou crie um backup sob demanda.

   a. Crie um plano de backup e atribua recursos ao backup. Consulte Criar um backup programado.

   b. Como alternativa, crie um backup sob demanda. Consulte Criar um backup sob demanda.
3. Verifique se você criou o `AWSBackupDefaultServiceRole` em sua conta seguindo estas etapas:

   a. Aguarde alguns instantes. Para obter mais informações, consulte As alterações que eu faço nem sempre ficam imediatamente visíveis no Guia do usuário do AWS Identity and Access Management.

   b. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

   c. No menu de navegação esquerdo, escolha Perfis.

   d. Na caixa de pesquisa, digite `AWSBackupDefaultServiceRole`. Se essa seleção existir, você criou a função AWS Backup padrão e concluiu esse procedimento.

   e. Se `AWSBackupDefaultServiceRole` ainda não for exibido, adicione as seguintes permissões ao usuário do IAM ou ao perfil do IAM que você usa para acessar o console.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource":"arn:aws:iam::*:role/service-role/AWSBackupDefaultServiceRole"
    },
    {
      "Effect":"Allow",
      "Action":[
        "iam:ListRoles"
```

```
      ],
      "Resource":"*"
    }
  ]
}
```

Para as regiões da China, substitua *aws* por *aws-cn*. Para AWS GovCloud (US) regiões, substitua *aws* por *aws-us-gov*.

f. Se não puder adicionar permissões ao seu usuário do IAM ou perfil do IAM, peça ao administrador que crie manualmente um perfil com um nome diferente de `AWSBackupDefaultServiceRole` e anexe esse perfil a estas políticas gerenciadas:

- `AWSBackupServiceRolePolicyForBackup`
- `AWSBackupServiceRolePolicyForRestores`

Políticas gerenciadas para AWS Backup

As políticas gerenciadas são políticas autônomas baseadas em identidade que você pode anexar a vários usuários, grupos e funções em seu. Conta da AWS Ao anexar uma política a uma entidade principal, você atribui à entidade as permissões que estão definidas na política.

AWS as políticas gerenciadas são criadas e administradas por AWS. Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada.

As políticas gerenciadas pelo cliente oferecem controles refinados para configurar o acesso aos backups. AWS Backup Por exemplo, você pode usá-los para fornecer ao administrador de backup do banco de dados acesso aos backups do Amazon RDS, mas não aos do Amazon EFS.

Para obter mais informações, consulte Políticas gerenciadas no Guia do usuário do IAM.

AWS políticas gerenciadas

AWS Backup fornece as seguintes políticas AWS gerenciadas para casos de uso comuns. Essas políticas facilitam a definição das permissões corretas e o controle de acesso aos seus backups. Existem dois tipos de políticas gerenciadas. Um tipo é projetado para ser atribuído aos usuários a fim de controlar o acesso ao AWS Backup. O outro tipo de política gerenciada foi projetado para

ser anexada às funções que você transmitir para o AWS Backup. A tabela a seguir lista todas as políticas gerenciadas que o AWS Backup fornece e descreve como elas são definidas. Você pode encontrar essas políticas gerenciadas na seção Políticas do console do IAM.

Políticas

- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

AWSBackupAuditAccess

Essa política concede permissões para que os usuários criem controles e estruturas que definam suas expectativas em relação a AWS Backup recursos e atividades e auditem AWS Backup recursos e atividades em relação aos controles e estruturas definidos. Essa política concede permissões AWS Config e serviços similares para descrever as expectativas do usuário e realizar as auditorias.

Essa política também concede permissões para entregar relatórios de auditoria ao Amazon S3 e a serviços similares e permite que os usuários encontrem e abram os relatórios de auditoria.

Para ver as permissões dessa política, consulte AWSBackupAuditAccessna Referência de política AWS gerenciada.

AWSBackupDataTransferAccess

Essa política fornece permissões para as APIs de transferência de dados do plano de AWS Backup armazenamento, permitindo que o agente AWS Backint conclua a transferência de dados de backup com o plano AWS Backup de armazenamento. Você pode vincular essa política às funções assumidas pelas instâncias do Amazon EC2 que executam o SAP HANA com o agente Backint.

Para ver as permissões dessa política, consulte AWSBackupDataTransferAccessna Referência de política AWS gerenciada.

AWSBackupFullAccess

O administrador de backup tem acesso total às AWS Backup operações, incluindo a criação ou edição de planos de backup, a atribuição de AWS recursos aos planos de backup e a restauração de backups. Os administradores de backup são responsáveis por determinar e aplicar a conformidade de backup definindo planos de backup que atendem aos requisitos regulamentares e empresariais da organização. Os administradores de backup também garantem que os AWS recursos de sua organização sejam atribuídos ao plano apropriado.

Para ver as permissões dessa política, consulte AWSBackupFullAccessna Referência de política AWS gerenciada.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Para ver as permissões dessa política, consulte na Referência de política AWS gerenciada.

AWSBackupOperatorAccess

Os operadores de backup são usuários que devem assegurar que os recursos aos quais eles são responsáveis são submetidos corretamente ao backup. Os operadores de backup têm permissões para atribuir AWS recursos aos planos de backup criados pelo administrador de backup. Eles também têm permissões para criar backups sob demanda de seus AWS recursos e configurar o período de retenção dos backups sob demanda. Operadores de backup não têm permissões para criar ou editar planos de backup ou excluir os backups programados depois de serem criados. Os operadores de backup podem restaurar backups. Você pode limitar os tipos de recursos que um operador de backup pode atribuir a um plano de backup ou de restauração a partir de um backup. Você faz isso permitindo que somente determinadas funções de serviço sejam passadas para AWS Backup quem tenha permissões para um determinado tipo de recurso.

Para ver as permissões dessa política, consulte AWSBackupOperatorAccessna Referência de política AWS gerenciada.

AWSBackupOrganizationAdminAccess

O administrador da organização tem acesso total às AWS Organizations operações, incluindo criação, edição ou exclusão de políticas de backup, atribuição de políticas de backup a contas e unidades organizacionais e monitoramento de atividades de backup dentro da organização. Os administradores da organização são responsáveis por proteger as contas na organização, definindo e atribuindo políticas de backup que atendam aos requisitos normativos e comerciais de sua organização.

Para ver as permissões dessa política, consulte AWSBackupOrganizationAdminAccessna Referência de política AWS gerenciada.

AWSBackupRestoreAccessForSAPHANA

Essa política fornece AWS Backup permissão para restaurar um backup do SAP HANA no Amazon EC2.

Para ver as permissões dessa política, consulte AWSBackupRestoreAccessForSAPHANAna Referência de política AWS gerenciada.

AWSBackupServiceLinkedRolePolicyForBackup

Essa política está anexada à função vinculada ao serviço chamada AWSServiceRoleforBackup para permitir AWS Backup a chamada de AWS serviços em seu nome para gerenciar seus backups. Para ter mais informações, consulte the section called “Backup e cópia”.

Para ver as permissões dessa política, consulte AWSBackupServiceLinkedRolePolicyforBackupna Referência de política AWS gerenciada.

AWSBackupServiceLinkedRolePolicyForBackupTest

Para ver as permissões dessa política, consulte AWSBackupServiceLinkedRolePolicyForBackupTestna Referência de política AWS gerenciada.

AWSBackupServiceRolePolicyForBackup

Fornece AWS Backup permissões para criar backups de todos os tipos de recursos compatíveis em seu nome.

Para ver as permissões dessa política, consulte AWSBackupServiceRolePolicyForBackupna Referência de política AWS gerenciada.

AWSBackupServiceRolePolicyForRestores

Fornece AWS Backup permissões para restaurar backups de todos os tipos de recursos compatíveis em seu nome.

Para ver as permissões dessa política, consulte AWSBackupServiceRolePolicyForRestoresna Referência de política AWS gerenciada.

Para restaurações de instâncias do EC2, inclua também as seguintes permissões para executar a instância do EC2:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/role-name",
            "Effect": "Allow"
        }
    ]
}
```

AWSBackupServiceRolePolicyForS3Backup

Essa política contém as permissões necessárias para AWS Backup fazer backup de qualquer bucket do S3. Isso inclui acesso a todos os objetos em um bucket e a qualquer AWS KMS chave associada.

Para ver as permissões dessa política, consulte AWSBackupServiceRolePolicyForS3Backupna Referência de política AWS gerenciada.

AWSBackupServiceRolePolicyForS3Restore

Essa política contém as permissões necessárias AWS Backup para restaurar um backup do S3 em um bucket. Isso inclui permissões de leitura e gravação nos buckets e o uso de qualquer AWS KMS chave em relação às operações do S3.

Para ver as permissões dessa política, consulte AWSBackupServiceRolePolicyForS3Restorena Referência de política AWS gerenciada.

AWSServiceRolePolicyForBackupReports

AWS Backup usa essa política para a função AWSServiceRoleForBackupReportsvinculada ao serviço. Essa função vinculada ao serviço fornece AWS Backup permissões para monitorar e relatar a conformidade de suas configurações, tarefas e recursos de backup com suas estruturas.

Para ver as permissões dessa política, consulte AWSServiceRolePolicyForBackupReportsna Referência de política AWS gerenciada.

AWSServiceRolePolicyForBackupRestoreTesting

Para ver as permissões dessa política, consulte AWSServiceRolePolicyForBackupRestoreTestingna Referência de política AWS gerenciada.

Políticas gerenciadas pelo cliente

As seções a seguir descrevem as permissões recomendadas de backup e restauração para o aplicativo Serviços da AWS e para o aplicativo de terceiros suportado pelo AWS Backup. Você pode usar as políticas AWS gerenciadas existentes como modelo ao criar seus próprios documentos de política e depois personalizá-los para restringir ainda mais o acesso aos seus AWS recursos.

Amazon Aurora

Backup

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurar

Comece com a `RDSPermissions` declaração de AWSBackupServiceRolePolicyForRestores.

Amazon DynamoDB

Backup

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForBackup:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`
- `KMSDynamoDBPermissions`

Restaurar

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForRestores:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamoDBRestorePermissions`
- `KMSPermissions`

Amazon EBS

Backup

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForBackup:

- `EBSResourcePermissions`
- `EBSTagAndDeletePermissions`
- `EBSCopyPermissions`
- `EBSSnapshotTierPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurar

Comece com a `EBSPermissions` declaração de AWSBackupServiceRolePolicyForRestores.

Adicione a instrução a seguir.

```
{
      "Effect":"Allow",
      "Action": [
```

```
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
},
```

Amazon EC2

Backup

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForBackup:

- `EBSCopyPermissions`
- `EC2CopyPermissions`
- `EC2Permissions`
- `EC2TagPermissions`
- `EC2ModifyPermissions`
- `EBSResourcePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurar

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForRestores:

- `EBSPermissions`
- `EC2DescribePermissions`
- `EC2RunInstancesPermissions`
- `EC2TerminateInstancesPermissions`
- `EC2CreateTagsPermissions`

Adicione a instrução a seguir.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
```

```
},
```

Amazon EFS

Backup

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForBackup:

- `EFSPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurar

Comece com a `EFSPermissions` declaração de AWSBackupServiceRolePolicyForRestores.

Amazon FSx

Backup

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForBackup:

- `FsxBackupPermissions`
- `FsxCreateBackupPermissions`
- `FsxPermissions`
- `FsxVolumePermissions`
- `FsxListTagsPermissions`
- `FsxDeletePermissions`
- `FsxResourcePermissions`
- `KMSPermissions`

Restaurar

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForRestores:

- `FsxPermissions`
- `FsxTagPermissions`
- `FsxBackupPermissions`

- `FsxDeletePermissions`
- `FsxDescribePermissions`
- `FsxVolumeTagPermissions`
- `FsxBackupTagPermissions`
- `FsxVolumePermissions`
- `DSPermissions`
- `KMSDescribePermissions`

Amazon RDS

Backup

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurar

Comece com a `RDSPermissions` declaração de AWSBackupServiceRolePolicyForRestores.

Amazon S3

Backup

Comece com AWSBackupServiceRolePolicyForS3Backup.

Adicione os `BackupVaultCopyPermissions` extratos `BackupVaultPermissions` e se precisar copiar os backups para uma conta diferente.

Restaurar

Comece com AWSBackupServiceRolePolicyForS3Restore.

AWS Storage Gateway

Backup

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForBackup:

- `StorageGatewayPermissions`
- `EBSTagAndDeletePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Adicione a instrução a seguir.

```
{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource":"*"
},
```

Restaurar

Comece com as seguintes declarações de AWSBackupServiceRolePolicyForRestores:

- `StorageGatewayVolumePermissions`
- `StorageGatewayGatewayPermissions`
- `StorageGatewayListPermissions`

Máquina virtual

Backup

Comece com a `BackupGatewayBackupPermissions` declaração de AWSBackupServiceRolePolicyForBackup.

Restaurar

Comece com a `GatewayRestorePermissions` declaração de AWSBackupServiceRolePolicyForRestores.

Backup criptografado

Para restaurar um backup criptografado, execute uma das seguintes ações:

- Adicione sua função à lista de permissões da política AWS KMS principal
- Adicione as seguintes declarações de AWSBackupServiceRolePolicyForRestoresà sua função do IAM para restaurações:
  - `KMSDescribePermissions`
  - `KMSPermissions`
  - `KMSCreateGrantPermissions`

Atualizações de políticas para AWS Backup

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Backup desde que esse serviço começou a rastrear essas alterações.

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup: atualizar para uma política existente	AWS Backup adicionou permissão `backup:TagResource` a esta política. A permissão é necessária para obter permissões de marcação durante a criação de um ponto de recuperação.	17 de maio de 2024
AWSBackupServiceRolePolicyForS3Backup: atualização para uma política existente	AWS Backup adicionou permissão `backup:TagResource` a esta política. A permissão é necessária para obter permissões de marcação durante a criação de um ponto de recuperação.	17 de maio de 2024

Alteração	Descrição	Data
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	AWS Backup adicionou permissão `backup:TagResource` a esta política. A permissão é necessária para obter permissões de marcação durante a criação de um ponto de recuperação.	17 de maio de 2024
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	A permissão foi adicionada `rds:DeleteDBInstanceAutomatedBackups`. Essa permissão é necessária para oferecer suporte AWS Backup ao backup contínuo e às instâncias point-in-time-restore do Amazon RDS.	1º de maio de 2024
AWSBackupFullAccess: atualização para uma política existente	AWS Backup atualizou o Amazon Resource Name (ARN) com permissão `storagegateway:ListVolumes` de `arn:aws:storagegateway:*:*:gateway/*` para para acomodar uma alteração * no modelo da API do Storage Gateway.	1º de maio de 2024

Alteração	Descrição	Data
AWSBackupOperatorAccess: atualização para uma política existente	AWS Backup atualizou o Amazon Resource Name (ARN) com permissão `storagegateway:ListVolumes` de `arn:aws:storagegateway:*:*:gateway/*` para para acomodar uma alteração * no modelo da API do Storage Gateway.	1º de maio de 2024

Alteração	Descrição	Data
AWSServiceRolePolicyForBackupRestoreTesting: atualização para uma política existente	Foram adicionadas as seguintes permissões para descrever e listar pontos de recuperação e recursos protegidos para realizar planos de teste de restauração: `backup:DescribeRecoveryPoint` `backup:DescribeProtectedResource` `backup:ListProtectedResources` ,, `backup:ListRecoveryPointsByResource` e. Foi adicionada a permissão `ec2:DescribeSnapshotTierStatus` para oferecer suporte ao armazenamento em nível de arquivamento do Amazon EBS. Foi adicionada a permissão `rds:DescribeDBClusterAutomatedBackups` para oferecer suporte aos backups contínuos do Amazon Aurora. Foram adicionadas as seguintes permissões para apoiar o teste de restauração dos backups do Amazon Redshift: e. `redshift:`	14 de fevereiro de 2024

Alteração	Descrição	Data
	`DescribeClusters` `redshift:DeleteClu ster` Foi adicionada a permissão `timestream:DeleteT able` para oferecer suporte ao teste de restauração dos backups do Amazon Timestream.	
AWSBackupServiceRo lePolicyForRestores: atualizaç ão para uma política existente	Foram adicionadas as permissões `ec2:Descr ibeSnapshotTierSta tus` `ec2:Resto reSnapshotTier` e. Essas permissões são necessárias para que os usuários tenham a opção de restaurar os recursos do Amazon EBS armazenad os a AWS Backup partir do armazenamento de arquivos. Para restaurações de instâncias do EC2, inclua também as permissões mostradas na seguinte declaração de política para inicializar a instância do EC2:	27 de novembro de 2023

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Foram adicionadas as permissões `ec2:DescribeSnapshotTierStatus` e oferecem suporte `ec2:ModifySnapshotTier` a uma opção de armazenamento adicional para que os recursos de backup do Amazon EBS sejam transferidos para o nível de armazenamento de arquivos. Essas permissões são necessárias para que os usuários tenham a opção de fazer a transição dos recursos do Amazon EBS armazenados AWS Backup para o armazenamento de arquivos.	27 de novembro de 2023

Alteração	Descrição	Data
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Foram adicionadas as permissões `ec2:DescribeSnapshotTierStatus` e oferecem suporte `ec2:ModifySnapshotTier` a uma opção de armazenamento adicional para que os recursos de backup do Amazon EBS sejam transferidos para o nível de armazenamento de arquivos. Essas permissões são necessárias para que os usuários tenham a opção de fazer a transição dos recursos do Amazon EBS armazenados AWS Backup para o armazenamento de arquivos. Foram adicionadas as permissões `rds:DescribeDBClusterSnapshots` `erds:RestoreDBClusterToPointInTime`, o que é necessário para PITR (point-in-time restaurações) dos clusters do Aurora.	

Alteração	Descrição	Data
AWSServiceRolePolicyForBackupRestoreTesting – Nova política	Fornece as permissões necessárias para realizar testes de restauração. As permissões incluem as ações `list, read, and write` para que os seguintes serviços sejam incluídos nos testes de restauração: 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 e Amazon S3.	27 de novembro de 2023
AWSBackupFullAccess: atualização para uma política existente	`restore-testing.backup.amazonaws.com` adicionado a `IamPassRolePermissions` e `IamCreateServiceLinkedRolePermissions`. Essa adição é necessária a AWS Backup para realizar testes de restauração em nome dos clientes.	27 de novembro de 2023

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foram adicionadas as permissões `rds:DescribeDBClusterSnapshots` e `rds:RestoreDBClusterToPointInTime`, o que é necessário para PITR (point-in-time restaurações) dos clusters do Aurora.	6 de setembro de 2023
AWSBackupFullAccess: atualização para uma política existente	Foi adicionada a permissão `rds:DescribeDBClusterAutomatedBackups`, que é necessária para backup e point-in-time restauração contínuos dos clusters Aurora.	6 de setembro de 2023
AWSBackupOperatorAccess: atualização para uma política existente	Foi adicionada a permissão `rds:DescribeDBClusterAutomatedBackups`, que é necessária para backup e point-in-time restauração contínuos dos clusters Aurora.	6 de setembro de 2023

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	A permissão foi adicionad `ards:DescribeDBClusterAutomatedBackups` . Essa permissão é necessária para AWS Backup oferecer suporte ao backup e point-in-time restauração contínuos dos clusters Aurora. Foi adicionada a permissão `rds:DeleteDBClusterAutomatedBackups` para permitir que o AWS Backup ciclo de vida exclua e desassocie os pontos de recuperação contínua do Amazon Aurora quando o período de retenção termina. Essa permissão é necessária para que o ponto de recuperação do Aurora evite a transição para um estado `EXIPIRED`. Foi adicionada a permissão `rds:ModifyDBCluster` que AWS Backup permite interagir com os clusters do Aurora. Essa adição permite que os usuários habilitem ou desabilitem backups contínuos com base nas configurações desejadas.	6 de setembro de 2023

Alteração	Descrição	Data
AWSBackupFullAccess: atualização para uma política existente	Foi adicionada a ação `ram:GetResourceShareAssociations` para conceder permissão ao usuário para obter associações de compartilhamento de recursos para o novo tipo de cofre.	8 de agosto de 2023
AWSBackupOperatorAccess: atualização para uma política existente	Foi adicionada a ação `ram:GetResourceShareAssociations` para conceder permissão ao usuário para obter associações de compartilhamento de recursos para o novo tipo de cofre.	8 de agosto de 2023
AWSBackupServiceRolePolicyForS3Backup: atualização para uma política existente	Foi adicionada a permissão `s3:PutInventoryConfiguration` para aprimorar as velocidades de desempenho de backup usando um inventário de buckets.	1º de agosto de 2023

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foram adicionadas as seguintes ações para conceder ao usuário permissões para adicionar tags `ec2:CreateTags` para restaurar recursos: `storagegateway:AddTagsToResource elasticfilesystem:TagResource` ,, pois somente `ec2:CreateAction` isso inclui `RunInstances` ou `CreateVolume fsx:TagResource` , `cloudformation:TagResource` e.	22 de maio de 2023
AWSBackupAuditAccess: atualização para uma política existente	Substituiu a seleção de recursos na API `config:DescribeComplianceByConfigRule` por um recurso curinga para facilitar a seleção de recursos pelo usuário.	11 de abril de 2023

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foi adicionada a seguinte permissão para restaurar o Amazon EFS usando uma chave gerenciada pelo cliente:`kms:GenerateDataKeyWithoutPlaintext` . Isso ajuda a garantir que os usuários tenham as permissões necessárias para restaurar os recursos do Amazon EFS.	27 de março de 2023
AWSServiceRolePolicyForBackupReports: atualização para uma política existente	As `config:DescribeConfigRuleEvaluationStatus` ações `config:DescribeConfigRules` e foram atualizadas para permitir que o AWS Backup Audit Manager acesse as regras gerenciadas pelo AWS Backup Audit Manager AWS Config .	9 de março de 2023

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForS3Restore: atualização para uma política existente	Foram adicionadas as seguintes permissões: `kms:Decrypt` `s3:PutBucketOwnershipControls` ,, e `s3:GetBucketOwnershipControls` à política `AWSBackupServiceRolePolicyForS3Restore` . Essas permissões são necessárias para compatibilidade com restaurações de objetos quando a criptografia do KMS é usada no backup original e para restaurar objetos quando a propriedade do objeto é configurada no bucket original em vez da ACL.	13 de fevereiro de 2023

Alteração	Descrição	Data
AWSBackupFullAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões para agendar backups usando tags VMware de máquinas virtuais e para oferecer suporte à limitação de largura de banda baseada em agendamento:`backup-gateway:GetHypervisorPropertyMappings` ,,,,, e. `backup-gateway:GetVirtualMachine` `backup-gateway:PutHypervisorPropertyMappings` `backup-gateway:GetHypervisor` `backup-gateway:StartVirtualMachinesMetadataSync` `backup-gateway:GetBandwidthRateLimitSchedule` `backup-gateway:PutBandwidthRateLimitSchedule`	15 de dezembro de 2022

Alteração	Descrição	Data
AWSBackupOperatorAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões para agendar backups usando tags VMware de máquinas virtuais e para oferecer suporte à limitação de largura de banda baseada em agendamento:,, e. `backup-gateway:GetHypervisorPropertyMappings` `backup-gateway:GetVirtualMachine` `backup-gateway:GetHypervisor` `backup-gateway:GetBandwidthRateLimitSchedule`	15 de dezembro de 2022
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync – Nova política	Fornece permissões para o AWS Backup Gateway sincronizar os metadados de máquinas virtuais em redes locais com o Backup Gateway.	15 de dezembro de 2022

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte às tarefas de backup do Timestream: `timestream:StartAwsBackupJob` `timestream:GetAwsBackupStatus` ,`timestream:ListTables` ,`timestream:ListDatabases` ,`timestream:ListTagsForResource` ,, `timestream:DescribeTable` `timestream:DescribeDatabase` , e. `timestream:DescribeEndpoints`	13 de dezembro de 2022

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte às tarefas de restauração do Timestream: `timestream:StartAwsRestoreJob` `timestream:GetAwsRestoreStatus` `timestream:ListTables` ,,`timestream:ListTagsForResource` ,`timestream:ListDatabases` ,`timestream:DescribeTable` ,, `timestream:DescribeDatabase` `s3:GetBucketAcl` , e. `timestream:DescribeEndpoints`	13 de dezembro de 2022
AWSBackupFullAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte aos recursos do Timestream: `timestream:ListTables` `timestream:ListDatabases` , e. `s3:ListAllMyBuckets` `timestream:DescribeEndpoints`	13 de dezembro de 2022

Alteração	Descrição	Data
AWSBackupOperatorAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte aos recursos do Timestream:`timestream:ListDatabases` , `timestream:ListTables` `s3:ListAllMyBuckets` , e. `timestream:DescribeEndpoints`	13 de dezembro de 2022
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte aos recursos do Timestream: `timestream:ListDatabases` `timestream:ListTables` ,`timestream:ListTagsForResource` ,`timestream:DescribeDatabase` ,`timestream:DescribeTable` ,, `timestream:GetAwsBackupStatus` `timestream:GetAwsRestoreStatus` , e. `timestream:DescribeEndpoints`	13 de dezembro de 2022

Alteração	Descrição	Data
AWSBackupFullAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte aos recursos do Amazon Redshift: `redshift:DescribeClusters redshift:DescribeClusterSubnetGroups ,redshift:DescribeNodeConfigurationOptions ,redshift:DescribeOrderableClusterOptions ,redshift:DescribeClusterParameterGroups ,, redshift:DescribeClusterTracks redshift:DescribeSnapshotSchedules` , e. `ec2:DescribeAddresses`	27 de novembro de 2022

Alteração	Descrição	Data
AWSBackupOperatorAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte aos recursos do Amazon Redshift: `redshift:DescribeClusters` ,,,`redshift:DescribeClusterSubnetGroups` ,`redshift:DescribeNodeConfigurationOptions` ,`redshift:DescribeOrderableClusterOptions` ,`redshift:DescribeClusterParameterGroups`, . `redshift:DescribeClusterTracks` `redshift:DescribeSnapshotSchedules` , `ec2:DescribeAddresses` e.	27 de novembro de 2022

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foram adicionadas as seguintes permissões para dar suporte às tarefas de restauração do Amazon Redshift: `redshift:RestoreFromCluster Snapshot` , `redshift:RestoreTableFromClusterSnapshot redshift:DescribeClusters` , e. `redshift:DescribeTableRestoreStatus`	27 de novembro de 2022
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte às tarefas de backup do Amazon Redshift: `redshift:CreateClusterSnapshot redshift:DescribeClusterSnapshots` ,`redshift:DescribeTags` ,, `redshift:DeleteClusterSnapshot redshift:DescribeClusters` , e. `redshift:CreateTags`	27 de novembro de 2022
AWSBackupFullAccess: atualização para uma política existente	Foi adicionada a seguinte permissão para oferecer suporte aos CloudFormation recursos:`cloudformation:ListStacks` .	27 de novembro de 2022

Alteração	Descrição	Data
AWSBackupOperatorAccess: atualização para uma política existente	Foi adicionada a seguinte permissão para oferecer suporte aos CloudFormation recursos:`cloudformation:ListStacks` .	27 de novembro de 2022
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Foram adicionadas as seguintes permissões aos CloudFormation recursos de suporte: `redshift:DescribeClusterSnapshots` `redshift:DescribeTags` `redshift:DeleteClusterSnapshot` ,, `redshift:DescribeClusters` e.	27 de novembro de 2022
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte às tarefas de backup da pilha de AWS CloudFormation aplicativos: `cloudformation:GetTemplate` `cloudformation:DescribeStacks` , e. `cloudformation:ListStackResources`	16 de novembro de 2022

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foram adicionadas as seguintes permissões para dar suporte às tarefas de backup da pilha de AWS CloudFormation aplicativos: `cloudformation:CreateChangeSet` e `cloudformation:DescribeChangeSet`	16 de novembro de 2022
AWSBackupOrganizationAdminAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões a essa política para permitir que os administradores da organização usem o recurso Administrador Delegado:`organizations:ListDelegatedAdministrator` ,, e `organizations:RegisterDelegatedAdministrator` `organizations:DeregisterDelegatedAdministrator`	27 de novembro de 2022

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte ao SAP HANA nas instâncias do Amazon EC2`ssm-sap:GetOperation` `ssm-sap:ListDatabases` `ssm-sap:BackupDatabase` `ssm-sap:UpdateHanaBackupSettings` `ssm-sap:GetDatabase` e `ssm-sap:ListTagsForResource`	20 de novembro de 2022
AWSBackupFullAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte ao SAP HANA nas instâncias do Amazon EC2`ssm-sap:GetOperation` `ssm-sap:ListDatabases` `ssm-sap:GetDatabase` e `ssm-sap:ListTagsForResource`	20 de novembro de 2022

Alteração	Descrição	Data
AWSBackupOperatorAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte ao SAP HANA nas instâncias do Amazon EC2`ssm-sap:GetOperation` :`ssm-sap:ListDatabases` ,`ssm-sap:GetDatabase` , e. `ssm-sap:ListTagsForResource`	20 de novembro de 2022
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Foi adicionada a seguinte permissão para oferecer suporte ao SAP HANA nas instâncias do Amazon EC2:. `ssm-sap:GetOperation`	20 de novembro de 2022
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foi adicionada a seguinte permissão para oferecer suporte a trabalhos de restauração do gateway de backup em uma instância EC2:`ec2:CreateTags` .	20 de novembro de 2022

Alteração	Descrição	Data
AWSBackupDataTransferAccess: atualização para uma política existente	Foram adicionadas as seguintes permissões para oferecer suporte à transferência segura de dados de armazenamento para recursos do SAP HANA no Amazon EC2`backup-storage:StartObject` :`backup-storage:PutChunk` ,`backup-storage:GetChunk` ,`backup-storage:ListChunks` ,, `backup-storage:ListObjects` `backup-storage:GetObjectMetadata` , e. `backup-storage:NotifyObjectComplete`	20 de novembro de 2022

Alteração	Descrição	Data
AWSBackupRestoreAccessForSAPHANA: atualização para uma política existente	Foram adicionadas as seguintes permissões para que os proprietários de recursos executem a restauração dos recursos do SAP HANA no 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` , e. `ssm-sap:ListTagsForResource`	20 de novembro de 2022
AWSBackupServiceRolePolicyForS3Backup: atualização para uma política existente	Foi adicionada a permissão `s3:GetBucketAcl` para oferecer suporte às operações de AWS Backup backup do Amazon S3.	24 de agosto de 2022

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foram adicionadas as seguintes ações para conceder acesso à criação de uma instância de banco de dados para oferecer suporte à funcionalidade Multi-Availability Zone (Multi-AZ):. `rds:CreateDBInstance`	20 de julho de 2022
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Foi adicionada a `s3:GetBucketTagging` permissão para conceder ao usuário permissão para selecionar buckets para backup com um curinga de recurso. Sem essa permissão, os usuários que selecionam quais buckets devem ser copiados com um caractere curinga de recurso não têm êxito.	6 de maio de 2022
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Foram adicionados recursos de volume no escopo das ações existentes `fsx:CreateBackup` e adicionadas novas `fsx:ListTagsForResource` ações `fsx:DescribeVolumes` para oferecer suporte ao FSx para backups em nível de volume do ONTAP.	27 de abril de 2022

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foram adicionadas as seguintes ações para conceder aos usuários permissões para restaurar FSx para volumes ONTAP`fsx:DescribeVolumes` ,`fsx:CreateVolumeFromBackup` , e. `fsx:DeleteVolume` `fsx:UntagResource`	27 de abril de 2022
AWSBackupServiceRolePolicyForS3Backup: atualização para uma política existente	Foram adicionadas as seguintes ações para conceder ao usuário permissões para receber notificações de alterações em seus buckets do Amazon S3 durante as operações de backup: e. `s3:GetBucketNotification` `s3:PutBucketNotification`	25 de fevereiro de 2022

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForS3Backup – Nova política	Foram adicionadas as seguintes ações para conceder ao usuário permissões para fazer backup de seus buckets do Amazon S3:`s3:GetInventoryConfiguration` ,,,`s3:PutInventoryConfiguration` ,`s3:ListBucketVersions` ,`s3:ListBucket` ,, `s3:GetBucketTagging` `s3:GetBucketVersioning` , e `s3:GetBucketNotification` `s3:GetBucketLocation` `s3:ListAllMyBuckets` Foram adicionadas as seguintes ações para conceder ao usuário permissões para fazer backup de seus objetos do Amazon S3:`s3:GetObject` ,`s3GetObjectAcl` ,`s3:GetObjectVersionTagging` , `s3:GetObjectVersionAcl` `s3:GetObjectTagging` , e. `s3:GetObjectVersion` Foram adicionadas as seguintes ações para conceder ao usuário permissões para fazer backup	17 de fevereiro de 2022

Alteração	Descrição	Data
	de seus dados criptografados do Amazon S3: e. `kms:Decrypt` `kms:DescribeKey` Foram adicionadas as seguintes ações para conceder ao usuário permissões para fazer backups incrementais de seus dados do Amazon S3 usando as regras EventBridge da Amazon`events:DescribeRule` : `events:EnableRule` `events:PutRule` ,`events:DeleteRule` ,`events:PutTargets` ,,`events:RemoveTargets` ,`events:ListTargetsByRule` , `events:DisableRule` `cloudwatch:GetMetricData` , e. `events:ListRules`	

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForS3Restore – Nova política	Foram adicionadas as seguintes ações para conceder ao usuário permissões para restaurar seus buckets do Amazon S3:`s3:CreateBucket` ,,`s3:ListBucketVersions` , `s3:ListBucket` `s3:GetBucketVersioning` , e. `s3:GetBucketLocation` `s3:PutBucketVersioning` Foram adicionadas as seguintes ações para conceder ao usuário permissões para restaurar seus buckets do Amazon S3:`s3:GetObject` ,`s3:GetObjectVersion` ,`s3:DeleteObject` ,`s3:PutObjectVersionAcl` ,,`s3:GetObjectVersionAcl` ,`s3:GetObjectTagging` ,`s3:PutObjectTagging` , `s3:GetObjectAcl` `s3:PutObjectAcl` , e. `s3:PutObject` `s3:ListMultipartUploadParts`	17 de fevereiro de 2022

Alteração	Descrição	Data
	Foram adicionadas as seguintes ações para conceder ao usuário permissões para criptografar seus dados restaurados do Amazon S3 `kms:Decrypt` , `kms:DescribeKey` , e `kms:GenerateDataKey`	
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Adicionado `s3:ListAllMyBuckets` para conceder ao usuário permissões para visualizar uma lista de seus buckets e escolher quais atribuir a um plano de backup.	14 de fevereiro de 2022
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Adicionado `backup-gateway:ListVirtualMachines` para conceder ao usuário permissões para visualizar uma lista de suas máquinas virtuais e escolher quais delas atribuir a um plano de backup. Adicionado `backup-gateway:ListTagsForResource` para conceder ao usuário permissões para listar as tags de suas máquinas virtuais.	30 de novembro de 2021

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Adicionado `backup-gateway:Backup` para conceder permissões ao usuário para restaurar seus backups de máquinas virtuais. AWS Backup também foi adicionado `backup-gateway:ListTagsForResource` para conceder ao usuário permissões para listar as tags atribuídas aos backups de suas máquinas virtuais.	30 de novembro de 2021
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Adicionado `backup-gateway:Restore` para conceder permissões ao usuário para restaurar seus backups de máquinas virtuais.	30 de novembro de 2021

Alteração	Descrição	Data
AWSBackupFullAccess: atualização para uma política existente	Foram adicionadas as seguintes ações para conceder aos usuários permissões para usar o AWS Backup Gateway para fazer backup, restaurar e gerenciar suas máquinas virtuais: `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:TestHypervisorConfigu`	30 de novembro de 2021

Alteração	Descrição	Data
	`ration ,backup-gateway:UntagResource ,backup-gateway:UpdateGatewayInformation ,, backup-gateway:UpdateHypervisor e.`	
AWSBackupOperatorAccess: atualização para uma política existente	Foram adicionadas as seguintes ações para conceder permissões ao usuário para fazer backup de suas máquinas virtuais: `backup-gateway:ListGateways backup-gateway:ListHypervisors backup-gateway:ListTagsForResource ,, backup-gateway:ListVirtualMachines e.`	30 de novembro de 2021
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Adicionado `dynamodb:ListTagsOfResource` para conceder ao usuário permissões para listar tags de suas tabelas do DynamoDB para backup usando os recursos avançados de backup AWS Backup do DynamoDB.	23 de novembro de 2021

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Adicionado `dynamodb:StartAwsBackupJob` para conceder ao usuário permissões para fazer backup de suas tabelas do DynamoDB usando recursos avançados de backup. Adicionado `dynamodb:ListTagsOfResource` para conceder ao usuário permissões para copiar tags de suas tabelas de origem do DynamoDB para seus backups.	23 de novembro de 2021
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Adicionado `dynamodb:RestoreTableFromAwsBackup` para conceder permissões ao usuário para restaurar o backup de suas tabelas do DynamoDB usando os recursos avançados AWS Backup de backup do DynamoDB.	23 de novembro de 2021
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Adicionado `dynamodb:RestoreTableFromAwsBackup` para conceder permissões ao usuário para restaurar o backup de suas tabelas do DynamoDB usando os recursos avançados AWS Backup de backup do DynamoDB.	23 de novembro de 2021

Alteração	Descrição	Data
AWSBackupOperatorAccess: atualização para uma política existente	As ações foram removidas `backup:GetRecoveryPointRestoreMetadata` e `rds:DescribeDBSnapshots` porque elas eram redundantes. AWS Backup não precisava de ambos `backup:GetRecoveryPointRestoreMetadata` e `backup:Get*` como parte de`AWSBackupOperatorAccess` . Além disso, AWS Backup não precisava de ambos `rds:DescribeDBSnapshots` e `rds:describeDBSnapshots` como parte de`AWSBackupOperatorAccess` .	23 de novembro de 2021

Alteração	Descrição	Data
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Foram adicionadas as novas ações `elasticfilesystem:DescribeFileSystems` `dynamodb:ListTables` ,`storagegateway:ListVolumes` ,`ec2:DescribeVolumes` ,`ec2:DescribeInstances` ,`rds:DescribeDBInstances` ,`rds:DescribeDBClusters` , e `fsx:DescribeFileSystems` para permitir que os clientes visualizem e escolham em uma lista AWS Backup de seus recursos suportados ao selecionar quais recursos atribuir a um plano de backup.	10 de novembro de 2021
AWSBackupAuditAccess – Nova política	Adicionado `AWSBackupAuditAccess` para conceder ao usuário permissões para usar o AWS Backup Audit Manager. As permissões incluem a possibilidade de configurar frameworks de conformidade e gerar relatórios.	24 de agosto de 2021

Alteração	Descrição	Data
AWSServiceRolePolicyForBackupReports – Nova política	Adicionado `AWSServiceRolePolicyForBackupReports` para conceder permissões para uma função vinculada ao serviço para automatizar o monitoramento de configurações, tarefas e recursos de backup para fins de conformidade com estruturas configuradas pelo usuário.	24 de agosto de 2021
AWSBackupFullAccess: atualização para uma política existente	Adicionado `iam:CreateServiceLinkedRole` para criar uma função vinculada ao serviço (com base no melhor esforço) para automatizar a exclusão de pontos de recuperação expirados para você. Sem essa função vinculada ao serviço, AWS Backup não é possível excluir pontos de recuperação expirados depois que os clientes excluem a função original do IAM que usaram para criar seus pontos de recuperação.	5 de julho de 2021

Alteração	Descrição	Data
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Foi adicionada a nova ação `dynamodb:DeleteBackup` para conceder `DeleteRecoveryPoint` permissão para automatizar a exclusão de pontos de recuperação expirados do DynamoDB com base nas configurações do ciclo de vida do seu plano de backup.	5 de julho de 2021
AWSBackupOperatorAccess: atualização para uma política existente	As ações foram removidas `backup:GetRecoveryPointRestoreMetadata` e `rds:DescribeDBSnapshots` porque elas eram redundantes. AWS Backup não precisava de ambos `backup:GetRecoveryPointRestoreMetadata` e, `backup:Get*` como parte de `AWSBackupOperatorAccess` Além disso, AWS Backup não precisava de ambos `rds:DescribeDBSnapshots` e `rds:describeDBSnapshots` como parte de `AWSBackupOperatorAccess`	25 de maio de 2021

Alteração	Descrição	Data
AWSBackupOperatorAccess: atualização para uma política existente	As ações foram removidas `backup:GetRecoveryPointRestoreMetadata` e `rds:DescribeDBSnapshots` porque elas eram redundantes. AWS Backup não precisava de ambos `backup:GetRecoveryPointRestoreMetadata` e `backup:Get*` como parte de`AWSBackupOperatorAccess` . Além disso, AWS Backup não precisava de ambos `rds:DescribeDBSnapshots` e `rds:describeDBSnapshots` como parte de`AWSBackupOperatorAccess` .	25 de maio de 2021
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foi adicionada a nova ação `fsx:TagResource` para conceder `StartRestoreJob` permissão para permitir que você aplique tags aos sistemas de arquivos Amazon FSx durante o processo de restauração.	24 de maio de 2021

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForRestores: atualização para uma política existente	Foram adicionadas as novas ações `ec2:DescribeImages` e `ec2:DescribeInstances` concederam `StartRestoreJob` permissão para permitir que você restaure instâncias do Amazon EC2 a partir de pontos de recuperação.	24 de maio de 2021
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Foi adicionada a nova ação `fsx:CopyBackup` para conceder `StartCopyJob` permissão para permitir que você copie os pontos de recuperação do Amazon FSx entre regiões e contas.	12 de abril de 2021
AWSBackupServiceLinkedRolePolicyForBackup: atualização para uma política existente	Foi adicionada a nova ação `fsx:CopyBackup` para conceder `StartCopyJob` permissão para permitir que você copie os pontos de recuperação do Amazon FSx entre regiões e contas.	12 de abril de 2021

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup: atualização para uma política existente	Atualizado para atender aos seguintes requisitos: AWS Backup Para criar um backup de uma tabela criptografada do DynamoDB, você deve adicionar `kms:Decrypt` as permissões `kms:GenerateDataKey` e a função do IAM usada para backup.	10 de março de 2021

Alteração	Descrição	Data
AWSBackupFullAccess: atualização para uma política existente	Atualizado para atender aos seguintes requisitos: Para usar AWS Backup para configurar backups contínuos para seu banco de dados do Amazon RDS, verifique se a permissão da API `rds:ModifyDBInstance` existe na função do IAM definida pela configuração do seu plano de backup. Para restaurar os backups contínuos do Amazon RDS, é necessário adicionar a permissão `rds:RestoreDBInstanceToPointInTime` ao perfil do IAM enviado para o trabalho de restauração. No AWS Backup console, para descrever o intervalo de vezes disponível para point-in-time recuperação, você deve incluir a permissão da `rds:DescribeDBInstanceAutomatedBackups` API em sua política gerenciada pelo IAM.	10 de março de 2021

Alteração	Descrição	Data
AWS Backup começou a rastrear as alterações	AWS Backup começou a rastrear as mudanças em suas políticas AWS gerenciadas.	10 de março de 2021

Usar perfis vinculados a serviço do AWS Backup

AWS Backup usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS Backup As funções vinculadas ao serviço são predefinidas AWS Backup e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Tópicos

- Usando funções para fazer backup e copiar
- Usando funções para o AWS Backup Audit Manager
- Usar perfis para testes de restauração

Usando funções para fazer backup e copiar

AWS Backup usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS Backup As funções vinculadas ao serviço são predefinidas AWS Backup e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração AWS Backup porque você não precisa adicionar manualmente as permissões necessárias. AWS Backup define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS Backup pode assumir suas funções. As permissões definidas incluem as políticas de confiança e de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus AWS Backup recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços suportados por funções vinculadas a serviços, consulte Serviços da AWS Suportados pelo IAM e procure os serviços que apresentarem Sim na coluna Função Vinculada a Serviço.. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculadas ao serviço para AWS Backup

AWS Backup usa a função vinculada ao serviço chamada AWSServiceRoleForBackup— Fornece AWS Backup permissões para listar recursos dos quais você pode fazer backup e copiar backups.

AWS Backup também usa a função para excluir todos os backups de todos os tipos de recursos, exceto do Amazon EC2.

A função AWSServiceRoleForBackup vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `backup.amazonaws.com`

Para ver as permissões dessa política, consulte AWSBackupServiceLinkedRolePolicyforBackupna Referência de política AWS gerenciada.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Crie uma função vinculada ao serviço para o AWS Backup

Não é necessário criar manualmente uma função vinculada a serviço. Quando você lista recursos para backup, configura o backup entre contas ou executa backups na AWS Management Console, na ou na AWS API AWS CLI, AWS Backup cria a função vinculada ao serviço para você.

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Para saber mais, consulte Uma Nova Função Apareceu na minha Conta do IAM.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta. Quando você lista recursos para backup,

configura o backup entre contas ou executa backups, AWS Backup cria a função vinculada ao serviço para você novamente.

Editar uma função vinculada ao serviço para o AWS Backup

AWS Backup não permite que você edite a função AWSServiceRoleForBackup vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Backup

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Limpar um perfil vinculado ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir qualquer recurso usado pelo perfil. Primeiro, você deve excluir todos os pontos de recuperação. Depois você deve excluir todos os cofres de backup.

> **Note**
>
> Se o AWS Backup serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir AWS Backup recursos usados pelo AWSServiceRoleForBackup (console)

1. Para excluir todos os pontos de recuperação e cofres de backup (exceto o cofre padrão), siga o procedimento em Excluir um cofre de backup.
2. Para excluir seu cofre padrão, use o seguinte comando na AWS CLI:

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

Para excluir AWS Backup recursos usados pelo AWSServiceRoleForBackup (AWS CLI)

1. Para excluir todos os seus pontos de recuperação, use delete-recovery-point.
2. Para excluir todos os cofres de backup, use `delete-backup-vault`.

Para excluir AWS Backup recursos usados pela AWSServiceRoleForBackup (API)

1. Para excluir todos os pontos de recuperação, use `DeleteRecoveryPoint`.
2. Para excluir todos os cofres de backup, use `DeleteBackupVault`.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForBackup vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas por funções vinculadas ao serviço do AWS Backup

AWS Backup suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Recursos e regiões compatíveis com o AWS Backup.

Usando funções para o AWS Backup Audit Manager

AWS Backup usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS Backup As funções vinculadas ao serviço são predefinidas AWS Backup e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração AWS Backup porque você não precisa adicionar manualmente as permissões necessárias. AWS Backup define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS Backup pode assumir suas funções. As permissões definidas incluem as políticas de confiança e de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus AWS Backup recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços suportados por funções vinculadas a serviços, consulte Serviços da AWS Suportados pelo IAM e procure os serviços que apresentarem Sim na coluna Função Vinculada a Serviço.. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculadas ao serviço para AWS Backup

AWS Backup usa a função vinculada ao serviço chamada AWSServiceRoleForBackupReports—AWS Backup Fornece permissão para criar controles, estruturas e relatórios.

A função AWSServiceRoleForBackupReports vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `backup.amazonaws.com`

Para ver as permissões dessa política, consulte AWSServiceRolePolicyForBackupReportsna Referência de política AWS gerenciada.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Crie uma função vinculada ao serviço para o AWS Backup

Não é necessário criar manualmente uma função vinculada a serviço. Quando você cria uma estrutura ou um plano de relatório na AWS Management Console, na ou na AWS API AWS CLI, AWS Backup cria a função vinculada ao serviço para você.

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Para saber mais, consulte Uma Nova Função Apareceu na minha Conta do IAM.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta. Quando você cria uma estrutura ou um plano de relatório, AWS Backup cria a função vinculada ao serviço para você novamente.

Editar uma função vinculada ao serviço para o AWS Backup

AWS Backup não permite que você edite a função AWSServiceRoleForBackupReports vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Backup

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Limpar um perfil vinculado ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir qualquer recurso usado pelo perfil. É necessário excluir todas as frameworks e todos os planos de relatório.

> **Note**
>
> Se o AWS Backup serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir AWS Backup recursos usados pelo AWSServiceRoleForBackupReports (console)

1. Como excluir todas as frameworks, consulte Excluir frameworks.
2. Como excluir todos os planos de relatório, consulte Excluir planos de relatório.

Para excluir AWS Backup recursos usados pelo AWSServiceRoleForBackupReports (AWS CLI)

1. Para excluir todos os frameworks, use delete-framework.
2. Para excluir todos os planos de relatório, use delete-report-plan.

Para excluir AWS Backup recursos usados pela AWSServiceRoleForBackupReports (API)

1. Para excluir todas as frameworks, use DeleteFramework.
2. Para excluir todos os planos de relatório, use DeleteReportPlan.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForBackupReports vinculada ao serviço. Para mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas por funções vinculadas ao serviço do AWS Backup

AWS Backup suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Recursos e regiões compatíveis com o AWS Backup.

Usar perfis para testes de restauração

AWS Backup usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS Backup As funções vinculadas ao serviço são predefinidas AWS Backup e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração AWS Backup porque você não precisa adicionar manualmente as permissões necessárias. AWS Backup define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS Backup pode assumir suas funções. As permissões definidas incluem as políticas de confiança e de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus AWS Backup recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços suportados por funções vinculadas a serviços, consulte Serviços da AWS Suportados pelo IAM e procure os serviços que apresentarem Sim na coluna Função Vinculada a Serviço.. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculadas ao serviço para AWS Backup

AWS Backup usa a função vinculada ao serviço chamada AWSServiceRolePolicyForBackupRestoreTesting— Fornece permissões de backup para realizar testes de restauração.

A função AWSServiceRolePolicyForBackupRestoreTesting vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `backup.amazonaws.com`

Para ver as permissões dessa política, consulte AWSServiceRolePolicyForBackupRestoreTestingna Referência de política AWS gerenciada.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Crie uma função vinculada ao serviço para o AWS Backup

Não é necessário criar manualmente uma função vinculada a serviço. Quando você realiza testes de restauração na AWS Management Console, na ou na AWS API AWS CLI, AWS Backup cria a função vinculada ao serviço para você.

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Para saber mais, consulte Uma Nova Função Apareceu na minha Conta do IAM.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta. Quando você realiza testes de restauração, AWS Backup cria a função vinculada ao serviço para você novamente.

Editar uma função vinculada ao serviço para o AWS Backup

AWS Backup não permite que você edite a função AWSServiceRolePolicyForBackupRestoreTesting vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o

nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Backup

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Limpar um perfil vinculado ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir qualquer recurso usado pelo perfil. É necessário excluir todos os planos de testes de restauração.

> **Note**
>
> Se o AWS Backup serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir AWS Backup recursos usados pelo AWSServiceRolePolicyForBackupRestoreTesting (console)

- Para excluir todos os planos de testes de restauração, consulte Testes de restauração.

Para excluir AWS Backup recursos usados pelo AWSServiceRolePolicyForBackupRestoreTesting (AWS CLI)

- Para excluir planos de testes de restauração, use `delete-restore-testing-plan`.

Para excluir AWS Backup recursos usados pela AWSServiceRolePolicyForBackupRestoreTesting (API)

- Para excluir planos de testes de restauração, use `DeleteRestoreTestingPlan`.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRolePolicyForBackupRestoreTesting vinculada ao serviço. Para mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas por funções vinculadas ao serviço do AWS Backup

AWS Backup suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Recursos e regiões compatíveis com o AWS Backup.

Prevenção contra o ataque do “substituto confuso” em todos os serviços

O problema “confused deputy” é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a personificação entre serviços pode resultar no problema do "substituto confuso". A imitação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado para utilizar as suas permissões para atuar nos recursos de outro cliente em que, de outra forma, ele não teria permissão para acessar. Para evitar isso, o AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos o uso das chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` nas políticas de recursos para limitar as permissões que AWS Backup concede a outro serviço para o recurso. Se você utilizar ambas as chaves de contexto de condição global, o valor `aws:SourceAccount` e a conta no valor `aws:SourceArn` deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

O valor de `aws:SourceArn` deve ser um cofre do AWS Backup ao usar o AWS Backup para publicar tópicos do Amazon SNS em seu nome.

A maneira mais eficaz de se proteger do problema ‘confused deputy’ é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se estiver especificando vários recursos, use a chave de condição de contexto global `aws:SourceArn` com curingas (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws::`*`servicename`*`::`*`123456789012`*`:*`.

Segurança da infraestrutura em AWS Backup

Como serviço gerenciado, AWS Backup é protegido pela segurança de rede AWS global. Para obter mais informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS Backup pela rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.2 ou posterior. Os clientes também devem ter suporte a pacotes de criptografia com sigilo de encaminhamento perfeito (PFS) como Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Diffie-Hellman Encaminhamento (ECDHE). A maioria dos sistemas modernos, como Java 7 e versões posteriores, suporta esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Integridade dos dados em AWS Backup

AWS Backup meta de integridade de dados

AWS Backup busca manter a integridade durante a transmissão, armazenamento e processamento de seus dados. AWS Backup trata os dados de recursos armazenados como informações críticas independentes do conteúdo, pois oferecemos o mesmo alto nível de segurança aos clientes, independentemente do tipo de dados que você armazena. Estamos atentos à segurança de nossos clientes e implementamos medidas técnicas e físicas sofisticadas contra o acesso não autorizado. Você mantém controle total sobre como seus dados são classificados, as regiões nas quais você armazena os dados e como você controla, arquiva e protege os dados contra divulgação.

AWS Backup implementação de integridade de dados

AWS Backup trabalha em conjunto com outros serviços AWS e com a Amazon para manter a integridade dos dados que armazena e com os quais interage. As ferramentas usadas podem variar e podem incluir (mas não estão limitadas a):

- Validação contínua de objetos em relação à soma de verificação para evitar a corrupção de objetos

- Somas de verificação internas para confirmar a integridade dos dados em trânsito e em repouso
- Somas de verificação calculadas com base nos dados em backups criados a partir do armazenamento primário
- Tentativa automática de restaurar os níveis normais de redundância do armazenamento de objetos em caso de corrupção do disco ou detecção de falha do dispositivo
- Armazenamento redundante de dados em vários locais físicos
- Aprimoramento da durabilidade do objeto em várias zonas de disponibilidade durante a gravação inicial, combinado com a replicação adicional no caso de indisponibilidade do dispositivo ou detecção de bit-rot
- Somas de verificação em todo o tráfego da rede, para detectar corrupção de pacotes de dados durante o armazenamento ou a recuperação dos dados.

AWS Backup armazena dados de forma nativa para o Amazon DynamoDB com recursos avançados, Amazon EFS, Amazon S3, Amazon Timestream e máquinas virtuais executadas com o VMware conectado por meio do gateway de Backup. AWS Backup facilita backups de dados armazenados com outros serviços, incluindo Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon FSx for Windows File Server, Amazon FSx for Lustre, Amazon FSx for OpenZFS, Amazon FSx for ONTAP, Amazon Neptune, Amazon RDS e Amazon Redshift. NetApp

Confirmação objetiva e auditoria da integridade dos dados do AWS Backup

Os dados armazenados diretamente pelo Amazon Simple Storage Service (Amazon S3) AWS Backup e os dados armazenados em parceria com outros AWS serviços com os quais AWS Backup interage estão sujeitos ao rigoroso processo do Amazon Simple Storage Service (Amazon S3) que sustenta essa integridade de dados. Essa integridade é confirmada por um auditor terceirizado independente por meio de um relatório anual de auditoria do SOC, disponível por meio do AWS Artifact no AWS Management Console;

Retenções legais e AWS Backup

A retenção legal é uma ferramenta administrativa que ajuda a evitar que os backups sejam excluídos enquanto estiverem em retenção. Enquanto a retenção estiver em vigor, não será possível excluir os backups em retenção, e as políticas de ciclo de vida que alterariam o status do backup (como a transição para o estado `Deleted`) serão adiadas até que a retenção legal seja removida. Um backup pode ter mais de uma retenção legal.

As retenções legais podem ser aplicadas a um ou mais backups (também conhecidos como pontos de recuperação) criados por, AWS Backup se seus ciclos de vida permitirem. Um tipo de backup chamado backup contínuo tem um ciclo de vida máximo de 35 dias. As retenções legais não estendem um ciclo de vida de backup contínuo.

Quando uma retenção legal é criada, ela pode levar em consideração critérios de filtragem específicos, como tipos de recursos e IDs de recursos. Além disso, é possível definir o intervalo de datas de criação dos backups que deseja incluir em uma retenção legal. As retenções legais e os backups têm uma relação de muitos: muitos, o que significa que um backup pode ter mais de uma retenção legal e uma retenção legal pode incluir mais de um backup. Cada conta pode ter um máximo de 50 retenções legais ativas ao mesmo tempo.

As retenções legais se aplicam somente ao backup original no qual foram colocadas. Quando um backup é copiado entre regiões ou contas (se o recurso for compatível com isso), ele não retém nem carrega consigo a retenção legal. Uma retenção legal, como outros recursos, tem um nome de recurso da Amazon (ARN) exclusivo associado a ela. Somente pontos de recuperação criados por AWS Backup podem fazer parte de uma retenção legal.

Observe que, embora o AWS Backup Vault Lock forneça proteções adicionais e imutabilidade a um cofre, uma retenção legal fornece proteção adicional contra a exclusão de backups individuais (pontos de recuperação). A retenção legal não expira e retém os dados no backup indefinidamente. A retenção permanece ativa até ser liberada por um usuário com permissões suficientes.

Criar uma retenção legal

Quando uma retenção legal é criada, ela contém somente pontos de recuperação que já foram criados. Backups (pontos de recuperação) com status de `EXPIRED` ou de `DELETING` não serão incluídos na retenção legal. Os pontos de recuperação (backups) com o status de `CREATING` podem não ser incluídos na retenção legal, dependendo do tempo de conclusão.

As retenções legais podem ser adicionadas por usuários que tenham as permissões necessárias do IAM.

Criar uma retenção legal usando o console do

Para criar uma retenção legal

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel à esquerda do console, encontre Minha conta. Escolha Retenções legais.

3. Escolha Adicionar retenção legal.
4. Três painéis são mostrados: detalhes da retenção legal, escopo da retenção legal e etiquetas de retenção legal.

    a. Em Detalhes da retenção legal, insira um título da retenção legal e uma descrição para a retenção nas caixas de texto fornecidas.
    b. No painel Escopo da retenção legal, escolha como você deseja selecionar o recurso a ser incluído na retenção. Ao criar uma retenção, você escolhe o método usado para selecionar os recursos que estão dentro da retenção legal. Você pode optar por incluir um dos seguintes:

        - Tipos de recursos e IDs específicos
        - Selecione cofres de backup
        - Todos os tipos de recursos ou todos os cofres de backup em sua conta

    c. Especificar o intervalo de datas da retenção legal. Insira as datas no formato AAAAA:MM:DD (as datas são inclusivas).
    d. Opcionalmente, você pode adicionar tags para a retenção em Tags de retenção legal. As tags podem ajudar a categorizar a retenção para referência e organização futuras. É possível adicionar até 50 tags no total.
5. Quando estiver satisfeito com a configuração da nova retenção legal, clique no botão Adicionar nova retenção.

Crie uma retenção legal usando o AWS CLI

Você pode criar uma retenção legal usando o create-legal-holdcomando.

```
aws backup create-legal-hold --title "my title" \
    --description "my description" \
    --recovery-point-selection
 "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

Visualizar retenções legais

Você pode ver os detalhes da retenção legal no AWS Backup console ou programaticamente.

Veja as retenções legais usando o console

Como visualizar todas as retenções legais em uma conta usando o console do Backup

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Usando a parte esquerda do painel, em Minha conta, clique em Retenções legais.
3. A tabela retenção legal exibe o título, o status, s descrição, o ID e a data de criação das retenções existentes. Clique no circunflexo (seta para baixo) ao lado do cabeçalho da tabela para filtrar a tabela pela coluna selecionada.

Visualizar retenções legais de forma programática

Para visualizar todas as retenções legais de forma programática, você pode usar as seguintes chamadas de API: e. ListLegalHoldsGetLegalHold

O modelo JSON a seguir pode ser usado 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
        }
   }
```

```
}
```

O modelo JSON a seguir pode ser usado 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,
  ]

}
```

A seguir estão os valores de status possíveis.

Status	Descrição
CRIANDO	Os pontos de recuperação solicitados estão em processo de retenção, e as solicitações de exclusão desses pontos de recuperação podem ter êxito, pois a retenção ainda não terminou de ser criada.
ACTIVE	A retenção legal foi criada. Todos os pontos de recuperação listados nessa retenção legal estão retidos.
CANCELAMENTO	As retenções legais estão em processo de remoção e as solicitações de exclusão dos pontos de recuperação sob a retenção podem ter êxito.
CANCELED	A retenção legal está totalmente liberada e não tem mais efeito. Os pontos de recuperação podem ser excluídos.

Liberar uma retenção legal

As retenções legais permanecem em vigor até serem removidas por um usuário com permissões suficientes. A remoção de uma retenção legal também é conhecida como cancelamento, exclusão ou liberação de uma retenção legal. A remoção de uma retenção legal a elimina de todos os backups aos quais ela foi anexada. Todos os backups que expiraram durante a retenção legal são excluídos dentro de 24 horas após a remoção da retenção legal.

Liberar uma retenção legal usando o console do

Para liberar uma suspensão usando o console

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Insira a descrição que você deseja associar à liberação.
3. Revise os detalhes e clique em Liberar retenção.

4. Quando a caixa de diálogo Liberar retenção for exibida, confirme sua intenção de liberar a retenção digitando `confirm` na caixa de texto.

    - Marque a caixa que confirma que você está cancelando a retenção.

Na página Retenções legais, é possível vier todas as suas retenções. Se a liberação tiver êxito, o status dessa retenção será mostrado como `Released`.

Libere uma retenção legal de forma programática

Para remover uma retenção programaticamente, use a chamada de API. CancelLegalHold

Use o modelo JSON a seguir.

```
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 permite que você estabeleça uma conexão privada entre sua nuvem privada virtual (“VPC”) e AWS Backup endpoints criando uma interface VPC endpoint. Os endpoints de interface são alimentados por AWS PrivateLinkuma tecnologia que permite que você acesse AWS Backup APIs de forma privada, restringindo todo o tráfego de rede entre sua VPC e AWS Backup a rede Amazon.

AWS PrivateLink permite que você acesse AWS Backup as operações de forma privada sem um gateway de internet, dispositivo NAT, conexão VPN ou AWS Direct Connect conexão. As instâncias em sua VPC não precisam de endereços IP públicos para se comunicar com os endpoints AWS Backup da API. Suas instâncias também não precisam de endereços IP públicos para usar nenhuma das operações disponíveis da API AWS Backup e da API do Backup Gateway. Tráfego entre sua VPC e AWS Backup não sai da rede Amazon.

Para obter mais informações sobre endpoints da VPC, consulte Endpoints da VPC de interface (AWS PrivateLink) no Guia do usuário da Amazon VPC.

Considerações sobre endpoints da Amazon VPC

Antes de configurar uma interface VPC endpoint para AWS Backup endpoints, revise as propriedades e limitações da interface endpoint no Guia do usuário da Amazon VPC.

Todas as AWS Backup operações relevantes para gerenciar os recursos do Amazon Backup estão disponíveis em sua VPC usando. AWS PrivateLink

As políticas de endpoint da VPC são compatíveis com endpoints do Backup. Por padrão, o acesso total às operações do Backup é permitido por meio do endpoint. Para obter mais informações, consulte Controlar o acesso a serviços com endpoints da VPC no Guia do usuário da Amazon VPC.

Criação de um AWS Backup VPC endpoint

Você pode criar um VPC endpoint para AWS Backup usar o console Amazon VPC ou o (CLI). AWS Command Line Interface AWS Para obter mais informações, consulte Criar um endpoint de interface no Manual do usuário da Amazon VPC.

Crie um VPC endpoint para AWS Backup usar o nome do serviço.
`com.amazonaws.region.backup`

Nas regiões China (Pequim) e China (Ningxia), o nome do serviço deve ser `cn.com.amazonaws.region.backup`.

Para endpoints do gateway de backup, use `com.amazonaws.region.backup-gateway`.

As seguintes portas TCP devem ser permitidas no grupo de segurança ao criar um endpoint da VPC para o gateway de backup:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Protocolo	Port	Direction	Origem	Destino	Uso
TCP	443 (HTTPS)	Saída	Gateway de backup	AWS	Para comunicação do Backup Gateway com o ponto final do AWS serviço

Usar um endpoint da VPC

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API AWS Backup com o endpoint VPC usando seu nome DNS padrão para a região, por exemplo. AWS `backup.us-east-1.amazonaws.com`

No entanto, para a região da China (Pequim) e a região da China (Ningxia) Regiões da AWS, as solicitações de API devem ser feitas com o VPC endpoint `backup.cn-north-1.amazonaws.com.cn` usando `backup.cn-northwest-1.amazonaws.com.cn` e, respectivamente.

Para obter mais informações, consulte Acessar um serviço por um endpoint de interface no Guia do usuário da Amazon VPC.

Criar uma política de endpoint da VPC

É possível anexar uma política de endpoint ao endpoint da VPC que controla o acesso à API do Amazon Backup. A política especifica:

- O principal que pode executar ações.
- As ações que podem ser executadas.
- Os recursos sobre os quais as ações podem ser realizadas.

> **Important**
>
> Quando uma política não padrão é aplicada a uma interface VPC endpoint, certas solicitações AWS Backup de API com falha, como aquelas que falharam, podem não ser `RequestLimitExceeded` registradas na Amazon. AWS CloudTrail CloudWatch

Para mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Exemplo: política de VPC endpoint para ações AWS Backup

Veja a seguir um exemplo de uma política de endpoint para AWS Backup. Quando anexada a um endpoint, essa política concede acesso às AWS Backup ações listadas para todos os princípios em todos os recursos.

```
{
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

Exemplo: política de endpoint da VPC que nega todo o acesso de uma conta da AWS especificada

A política de VPC endpoint a seguir nega à AWS conta `123456789012` todo o acesso aos recursos que usam o endpoint. A política permite todas as ações de outras contas.

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"Stmt1645236612384",
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

Para obter mais detalhes sobre as respostas de API disponíveis, consulte o Guia da API.

AWS Backup Atualmente, a disponibilidade oferece suporte a VPC endpoints nas seguintes regiões: AWS

- Região Leste dos EUA (Ohio)
- Região Leste dos EUA (N. da Virgínia)
- Região Oeste dos EUA (Oregon)
- Região Oeste dos EUA (Norte da Califórnia).
- Região África (Cidade do Cabo)
- Região Ásia-Pacífico (Hong Kong)
- Região Ásia-Pacífico (Mumbai)
- Região Ásia-Pacífico (Osaka)
- Região Ásia-Pacífico (Seul)
- Região Ásia-Pacífico (Singapura)

- Região Ásia-Pacífico (Sydney)
- Região Ásia-Pacífico (Tóquio)
- Região do Canadá (Central)
- Região Europa (Frankfurt)
- Região Europa (Irlanda)
- Região Europa (Londres)
- Região Europa (Paris)
- Região Europa (Estocolmo)
- Região Europa (Milão)
- Região Oriente Médio (Bahrein)
- Região América do Sul (São Paulo)
- Região Ásia-Pacífico (Jacarta)
- Região Ásia-Pacífico (Osaka)
- Região da China (Pequim)
- Região da China (Ningxia)
- AWS GovCloud (Leste dos EUA)
- AWS GovCloud (Oeste dos EUA)

> **Note**
>
> AWS Backup para VMware não está disponível nas regiões da China (região da China (Pequim) e região da China (Ningxia)) ou na região Ásia-Pacífico (Jacarta).

Resiliência em AWS Backup

AWS Backup leva sua resiliência — e sua segurança de dados — extremamente a sério.

AWS Backup armazena seus backups com pelo menos tanta resiliência e durabilidade quanto o AWS serviço original do seu recurso ofereceria, se você fizesse o backup lá.

AWS Backup foi projetado para usar a infraestrutura AWS global para replicar seus backups em várias zonas de disponibilidade para obter durabilidade de 99,999999999% (11 noves) em um determinado ano, desde que você siga a documentação atual. AWS Backup

AWS Backup criptografa seus planos de backup em repouso e os faz backup contínuo. Você também pode restringir o acesso aos seus planos de backup usando credenciais e políticas AWS Identity and Access Management (IAM). Para obter mais informações, consulte Autenticação, Controle de acesso e Práticas recomendadas de segurança no IAM.

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. AWS Backup armazena seus backups nas zonas de disponibilidade. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais. Para obter mais informações, consulte o Acordo de Serviço (SLA) do AWS Backup.

Além disso, AWS Backup permite que você copie seus backups em todas as regiões para obter uma resiliência ainda maior. Para obter mais informações sobre o recurso de cópia AWS Backup entre regiões, consulte Criando uma Cópia de Backup.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

AWS Backup cotas

As cotas a seguir se aplicam ao trabalhar com AWS Backup. Muitas AWS Backup cotas são ajustáveis se permitidas pelo serviço de tipo de recurso. Para solicitar um ajuste de cota, descreva seu caso de uso para o AWS Support.

AWS Backup cotas

Recurso	Cota	Observações
Número de cofres de backup por região por conta	300	É possível solicitar um ajuste.
Número de pontos de recuperação por cofre de backup	1.000.000	É possível solicitar um ajuste.
Número de planos de backup por região por conta	300	É possível solicitar um ajuste.
Número de versões por plano de backup	2.000	É possível solicitar um ajuste.
Número de atribuições de recurso por plano de backup	100	Não ajustável
Número de trabalhos de backup ativos por conta	Ilimitado	
Número de cópias de backup simultâneas por saída de conta para uma região de destino	100	É possível solicitar um ajuste para determinados recursos (atualmente máquinas virtuais, bancos de dados do Advanced DynamoDB, Timestream, Amazon EFS e SAP HANA em instâncias do Amazon EC2)

Recurso	Cota	Observações
Número de cópias simultâneas por cofre de backup de destino na conta após o limite (entrada acima) ter sido atingido	5	Não ajustável
Número de cópias simultâneas entre contas que podem ser feitas do mesmo recurso para a mesma região de destino	30	Não ajustável.
Número de trabalhos de backup e de cópia simultâneos por recurso	1	Não ajustável. Essa cota ajuda você a manter o desempenho de suas workloads.
Número de tags de metadados por backup	50	Você não pode solicitar um ajuste. AWS impõe essa cota em todos os recursos. Consulte os limites e requisitos de nomenclatura de tags na Referência geral da AWS .
Número de tags por seleção de recursos em uma política de backup entre contas	30	Não ajustável. Tags adicionais podem ser incluídas utilizando várias atribuições de recursos ou planos de backup.
Número de hipervisores	10	Não ajustável
Número de retenções legais	50 por conta	Não ajustável
Número máximo de camadas de backup aninhadas de pilhas de aplicações	10	Não ajustável

AWS Backup das cotas de recursos do Amazon Timestream

Recurso	Cota	Observações
Número de trabalhos simultâneos de backup do Timestream por conta	4	É possível solicitar um ajuste.
Número de trabalhos de restauração simultâneos do Timestream por conta	1	É possível solicitar um ajuste.

Há cotas em uma única atribuição de recursos em uma única regra de backup. É possível criar um plano de backup com várias regras de backup.

AWS Backup Cotas do Audit Manager

Recurso	Cota	Observações
Número de frameworks por conta por região	15	É possível solicitar um ajuste.
Número de controles por conta por região	50	É possível solicitar um ajuste.
Número de planos de relatório por conta	20	É possível solicitar um ajuste.
Número de frameworks por plano de relatório	1.000	Não ajustável
Número máximo de contas multiplicado por regiões em um plano de relatório	300	Não ajustável

Cotas dos planos de testes de restauração

Recurso	Cota	Observações
Planos de testes de restauração	100	Não ajustável
Número de etiquetas em cada plano	50	Não ajustável
Seleções por plano	30	Não ajustável
ARNs por seleção de testes de restauração	30	Não ajustável
Condições por seleção	30	Inclui aquelas contidas em `StringEquals` e `StringNotEquals`
Seletores de cofre por seleção de testes de restauração	30	Não ajustável
Valor máximo (em dias) da janela de seleção	365 dias	
Limites de horas para a janela de início	Mínimo: 1 hora; máximo: 168 horas	
Máximo de caracteres para o nome do plano dos testes de restauração	50 caracteres	Alfanuméricos e sublinhados, sem espaços em branco
Máximo de caracteres para o nome da seleção dos testes de restauração	50 caracteres	Alfanuméricos e sublinhados, sem espaços em branco

AWS Backup gateway cotas

Recurso	Cota	Observações
Trabalhos de backup ou de restauração por gateway	4	Não é possível solicitar um ajuste. Em vez disso, crie mais gateways e conecte-os ao seu hipervisor.

Ao gerenciar backups em várias contas usando AWS Organizations, você pode encontrar cotas AWS Organizations impostas. Para essas cotas, consulte Cotas para o AWS Organizations no Guia do usuário do AWS Organizations .

Você também pode encontrar cotas impostas por um serviço AWS Backup compatível, incluindo:

- Amazon Elastic File System
- Amazon Elastic Block Store
- 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

Monitoramento

AWS Backup trabalha com outras AWS ferramentas para permitir que você monitore suas cargas de trabalho. Essas ferramentas incluem o seguinte:

- AWS Backup painéis de console
  - O painel de trabalhos oferece monitoramento de integridade dos trabalhos, onde você pode visualizar métricas que mostram sucessos e fracassos de trabalhos, filtradas por motivos, contas, região e tipo de recurso.
  - O painel de trabalhos está disponível nas regiões em que o AWS Backup Audit Manager é suportado. Consulte Disponibilidade de recursos por Região da AWS para conferir essas regiões. Todas as outras regiões poderão acessar o CloudWatch Painel.
- Amazon CloudWatch e Amazon EventBridge para monitorar AWS Backup processos.
  - Você pode usar CloudWatch para monitorar métricas, criar alarmes e visualizar painéis.
  - Você pode usar EventBridge para visualizar e monitorar AWS Backup eventos.

  Para obter mais informações, consulte Monitorando AWS Backup eventos usando a Amazon EventBridge e .
- AWS CloudTrailpara monitorar chamadas de AWS Backup API. É possível identificar a hora, o IP de origem, os usuários e as contas que fazem essas chamadas. Para ter mais informações, consulte Registrando chamadas de AWS Backup API com CloudTrail.
- Amazon Simple Notification Service (Amazon SNS) para assinar tópicos AWS Backup relacionados, como eventos de backup, restauração e cópia. Para ter mais informações, consulte Opções de notificação com AWS Backup.

AWS Backup painéis de console

> **Note**
>
> O painel de empregos está disponível em todas as regiões em que o AWS Backup Audit Manager é suportado. Consulte Disponibilidade de recursos por Região da AWS para conferir essas regiões. Todas as outras regiões poderão acessar o CloudWatch Painel.

Tópicos

Visão geral dos painéis de backup

AWS Backup fornece um painel de tarefas no console para ajudá-lo a monitorar a integridade de suas tarefas de backup, cópia e restauração. Os mesmos dados exibidos visualmente no console podem ser recuperados na linha de comando por meio AWS CLI de.

O painel de trabalhos pode ser usado para identificar problemas em trabalhos de backup, cópia e restauração por meio do monitoramento de contas de membro ou de nível organizacional. Com essas informações, você pode identificar e diagnosticar eventos e possíveis problemas para ajudar a garantir a fidelidade em suas atividades.

O painel de trabalhos pode exibir dois períodos. Por padrão, são exibidos os dados dos últimos 14 dias, mas você pode alterar a exibição para mostrar os últimos 7 dias. Se você alterar o cronograma, os dados serão atualizados para refletir o novo intervalo de tempo.

Observe que o painel exibe dados até a 0h UTC mais recente, ou seja, os dados do dia atual não estão incluídos. O painel é atualizado diariamente por volta da 1h30 às 2h30 UTC.

Visualizar o painel de trabalhos

Para visualizar o painel de tarefas, faça login no AWS Backup console e selecione Painéis de tarefas na barra de navegação esquerda.

Na página do painel de trabalhos, você pode selecionar na guia de trabalhos de backup, cópia ou restauração.

A visão geral do painel de trabalhos exibe a visualização agregada ao longo do período especificado para a atividade de trabalhos, incluindo trabalhos concluídos, concluídos com problemas, expirados e trabalhos com falha. Por padrão, são exibidos os dados dos últimos 14 dias, mas você pode alterar a exibição para mostrar 7 dias.

> **Note**
>
> `Completed with issues` é o status de um trabalho exibido no console para indicar um trabalho concluído com uma mensagem de status.

Integridade do trabalho

O gráfico de linhas exibe as linhas de taxa de trabalhos bem-sucedidos e malsucedidos ao longo do tempo. A linha de taxa de sucesso mostra uma agregação dos trabalhos concluídos e concluídos com problemas. A linha de taxa de fracasso mostra a soma dos trabalhos com falha e expirados de acordo com o intervalo de tempo especificado.

Os trabalhos não concluídos ou sem falha (trabalhos com status de criado, pendente, em execução, anulado, anulando ou parcial) não são incluídos. A porcentagem total pode não ser igual a 100%.

Status do trabalho ao longo do tempo

Você pode gerar um gráfico de barras personalizado que mostra o número de trabalhos em cada categoria (Concluído, Concluído com problemas, Com falha e Expirado), distribuído por dias.

Com os menus suspensos, escolha os status, os tipos de recursos e AWS as regiões que você deseja ver no gráfico. Se você quiser explorar ainda mais sua seleção, escolha Exibir tarefas para ver uma parte pré-filtrada da página de monitoramento de trabalhos/contas cruzadas.

Você pode passar o mouse sobre uma barra para exibir um pop-over que mostra dados detalhados do trabalho para a data selecionada.

Trabalhos problemáticos

Um trabalho problemático é um trabalho que tem o status Com falha, Expirado ou Concluído com problemas. Cada gráfico exibe a métrica correspondente que contém as contas, os tipos de recurso ou os principais motivos que contêm o maior número de trabalhos problemáticos.

A exibição padrão classifica o widget do painel pela métrica especificada em ordem decrescente, começando pela métrica com o maior número de trabalhos problemáticos que pertencem à métrica.

A exibição das principais contas problemáticas só será visível em contas que tenham acesso por meio do Organizations, como contas administrativas e contas de administrador delegado. Se essa exibição estiver disponível, você poderá passar o mouse sobre uma conta para exibir o número de trabalhos problemáticos que pertencem à conta escolhida.

Você pode selecionar uma barra do gráfico para abrir uma janela pop-up. Nessa janela, você pode selecionar um status de trabalho para abrir uma tabela de monitoramento de trabalhos/contas cruzadas filtrada pelo status selecionado.

Motivos dos trabalhos problemáticos

O widget Principais motivos problemáticos mostra a categoria do código da mensagem à qual as mensagens de erro pertencem. No entanto, a categoria pode não explicar os problemas que um trabalho enfrenta. Expanda as categorias de código de mensagem abaixo para ver mais detalhes sobre as mensagens ou os erros específicos que os trabalhos podem estar enfrentando.

“VSS_ERROR”

- “A tentativa de backup do VSS do Windows falhou porque a instância ou o SSM Agent tem um estado inválido ou privilégios insuficientes.”
- “A tentativa de backup do VSS do Windows falhou devido a privilégios insuficientes para realizar essa operação.”
- “A tentativa de backup do VSS do Windows falhou porque o ec2-vss-agent.exe não está instalado na instância.”
- “Erro encontrado no trabalho de backup do VSS do Windows; tentando realizar um backup regular.”
- “A tentativa de backup do VSS do Windows falhou porque a criação de snapshots habilitados para VSS atingiu o tempo limite.”
- “A tentativa de backup do VSS do Windows falhou devido à versão incompatível do Windows Server. As versões compatíveis são o Windows Server 2012 e posteriores.”
- “A tentativa de backup do VSS do Windows falhou porque a criação de snapshots habilitados para VSS atingiu o tempo limite.”

"LIMIT_EXCEEDED"

- “Limite de assinante excedido: você atingiu o número máximo de backups simultâneos, que é 300. Aguarde a conclusão de outros trabalhos e tente novamente. Você também pode entrar em contato AWS Support para solicitar um aumento de cota.”
- “O máximo permitido de snapshots em andamento para um único volume foi excedido.”
- “O limite máximo de snapshots ativos permitidos foi excedido.”
- “Não é possível criar mais de 20 snapshots do usuário.”

- “O conjunto de etiquetas resultante não deve ter mais de 50 etiquetas de usuário.”
- “Você atingiu o máximo de backups compatíveis para sua conta/banco de dados. Para obter informações adicionais, consulte Cotas no Guia do desenvolvedor do Timestream.”
- “Você atingiu sua cota de 50.000 para o número de imagens públicas e privadas permitidas nesta região. Cancele o registro de imagens não utilizadas ou solicite um aumento da sua cota de AMI.”
- “Seu backup foi bem-sucedido, mas não conseguimos manter os NetworkInterfaces metadados, pois seu tamanho excedia nossos limites internos.”
- “REGEX#Limite de assinante excedido”
- “REGEX#Mais de 50 etiquetas especificadas”
- “REGEX#pode ter no máximo”

“ACCESS_DENIED”

- “Você não tem autorização para executar esta operação.”
- “Acesso negado ao tentar ligar para o AWS Backup serviço”
- “As imagens de AWS Marketplace não podem ser copiadas para outra AWS conta.”
- “O trabalho de cópia falhou porque o cofre de backup de destino está criptografado com a chave gerenciada do serviço de backup padrão. Não é possível copiar o conteúdo desse cofre. Somente o conteúdo de um cofre de Backup criptografado por uma AWS KMS chave pode ser copiado.
- Os instantâneos criptografados com o não Chave gerenciada pela AWS podem ser compartilhados. Especifique outro snapshot.”
- “Snapshots criptografados com a chave padrão do Amazon EBS não podem ser compartilhados.”
- “Falha no trabalho de cópia. As contas de origem e destino devem ser membros da mesma organização.”
- “REGEX#access negado”
- “REGEX#não tem autorização para”
- “REGEX #cannot seja assumido por AWS Backup
- “REGEX#não tem permissão”
- “REGEX#permissão ausente”

“CONCURRENT_JOB”

- “O trabalho de backup falhou porque havia um trabalho em execução para o mesmo recurso.”

“FEATURE_NOT_ENABLED”

- “Falha no trabalho de cópia. O recurso de cópia entre contas não está habilitado para a organização atual.”

“JOB_EXPIRED”

- “O trabalho de backup expirou antes da conclusão.”

“INVALID_LIFECYCLE”

- “Falha no trabalho de cópia. A retenção especificada no trabalho não está dentro do intervalo especificado para o cofre de backup de destino.”
- “REGEX#não foi possível iniciar porque está dentro ou muito próximo da janela de manutenção semanal configurada”
- “REGEX#não foi possível iniciar porque está dentro ou muito próximo da janela de backup automatizado configurada”

“INVALID_STATE”

- “REGEX#instância não está no estado”
- “REGEX#não está no estado disponível”
- “REGEX#não está no estado disponível”
- “REGEX#não é possível criar snapshot de volume”

“KMS_KEY_ERROR”

- “A chave do KMS está desabilitada ou com exclusão pendente, ou o acesso à chave do KMS foi negado.”
- “O ID de chave fornecido não está acessível.”
- “A cópia do snapshot da AMI falhou com o seguinte erro: O ID de chave fornecido não está acessível. Você deve ter DescribeKey permissões na CMK padrão”
- “REGEX#chave do kms”

“ACCESS_KEY_ERROR”

- “O ID da chave de AWS acesso precisa de uma assinatura para o serviço”

“HYPERVISOR_OFFLINE”

- “Essa operação não é válida para o hipervisor especificado porque não está on-line.”

“RESOURCE_NOT_FOUND”

- “O volume especificado não foi encontrado.”
- “A máquina virtual não foi encontrada.”
- “O ID de chave fornecido não existe.”
- “REGEX#não existe”
- “REGEX#não foi possível encontrar recurso”
- “REGEX#não foi possível encontrar cryopod”
- “REGEX#não foi possível encontrar ponto de recuperação”
- “REGEX#recurso não encontrado”
- “REGEX#não está mais disponível”
- “REGEX#é inválido”

“RESOURCE_NOT_SUPPORTED”

- “REGEX#tipo de recurso incompatível”
- “REGEX#tipo de recurso incompatível”

“TAG_COPY_ERROR”

- “Não foi possível copiar etiquetas de recursos para o backup devido a uma falha interna.”
- “Não foi possível copiar etiquetas de recursos para o backup porque o ponto de recuperação de origem ou destino não está disponível.”

“TOKEN_EXPIRED”

- “O token expirou. Tente novamente.”

“UNSUPPORTED_OPERATION”

- “CreateSnapshot método não suportado no hipervisor durante a criação do instantâneo. Trabalho de backup anulado.”
- “UnsupportedOperation : As cópias de backup do Storage Gateway exigem um cofre de backup criado pelo usuário e uma CMK no destino.”
- “REGEX#recurso incompatível com o tipo de recurso fornecido”

“FATAL_ERROR”

- “Ocorreu um erro interno.”
- “O trabalho de cópia encontrou um erro fatal. Entre em contato com AWS o Support para obter mais assistência.”
- “O trabalho de cópia encontrou um erro fatal.”
- “REGEX#o trabalho de cópia encontrou um erro fatal”

Obtendo dados do painel por meio de AWS CLI

Você pode usar a linha de comandos para recuperar os mesmos dados que aparecem no console. Use um dos seguintes comandos da CLI:

- `list-backup-job-summaries`
- `list-copy-job-summaries`
- `list-restore-job-summaries`

Estes são os parâmetros válidos que você pode incluir em 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)
```

Este exemplo mostra um exemplo de solicitação em que o usuário inseriu `list-backup-job-summaries` e a solicitação pede a devolução de todas as contas disponíveis com um estado `FAILED` desde antes dos últimos 14 dias:

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

Para obter uma contagem dos trabalhos com status `completed with issues`, subtraia a contagem de trabalhos `COMPLETED` com um `MessageCategory` de `SUCCESS` do número total de `COMPLETED`.

Monitorando AWS Backup eventos usando a Amazon EventBridge

AWS Backup envia eventos para a Amazon EventBridge quando o estado de uma tarefa de backup ou cópia muda. Você pode usar EventBridge para monitorar AWS Backup eventos. Por exemplo, você pode receber um alarme quando uma tarefa de backup falhar. AWS Backup emite eventos com o EventBridge melhor esforço a cada 5 minutos.

Para rastrear eventos usando EventBridge, veja o seguinte:

- Criação de uma regra que reage aos eventos (Amazon EventBridge User Guide)

- CloudWatch Eventos e métricas da Amazon para AWS Backup (blog - consulte Configurar AWS Backup eventos para enviar para a Amazon EventBridge)

Alguns eventos relatam`status: COMPLETED`, enquanto outros eventos relatam `state: COMPLETED`. Isso é consistente com a AWS Backup API. Alguns status são específicos do AWS Backup console: o status de `Completed with issues` status é uma representação de `Completed` trabalhos com mensagens de status. Para monitorar eventos `Completed with issues`, monitore trabalhos `COMPLETED` que tenham uma mensagem de status.

Como alternativa, você pode usar a API de AWS Backup notificação para rastrear AWS Backup eventos com o Amazon Simple Notification Service (Amazon SNS). No entanto, EventBridge rastreia mais alterações do que a API de notificação, incluindo alterações nos cofres de backup, no estado da tarefa de cópia, nas configurações da região e no número de pontos de recuperação frios ou quentes.

Eventos

- Eventos do Backup Job
- Eventos do Plano de Backup
- Eventos do Backup Vault
- Eventos de Copy Job
- Eventos de ponto de recuperação
- Eventos de configurações de região
- Eventos do Restore Job

Eventos do Backup Job

Veja a seguir exemplos de eventos.

State

- Estado: FALHOU
- Estado: CONCLUÍDO
- Estado: RUNNING
- Estado: ABORTED
- Estado: EXPIRADO

- Estado: PENDENTE
- Estado: CRIADO

Estado: FALHOU


```
{
  "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: CONCLUÍDO


```
{
  "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: RUNNING

```
{
  "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: ABORTED

```
{
  "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: EXPIRADO

```
{
  "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: PENDENTE


```
{
  "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: CRIADO


```
{
  "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 do Plano de Backup

Veja a seguir exemplos de eventos.

State

- Estado: MODIFICADO
- Estado: EXCLUÍDO
- Estado: CRIADO

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: EXCLUÍDO

```
{
  "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: CRIADO

```
{
  "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 do Backup Vault

Veja a seguir exemplos de eventos.

State

- Estado: CRIADO
- Estado: MODIFICADO
- Estado: EXCLUÍDO

Estado: CRIADO


```
{
  "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: EXCLUÍDO

```
{
  "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

Veja a seguir exemplos de eventos.

State

- Estado: FALHOU
- Estado: RUNNING
- Estado: CONCLUÍDO
- Estado: CRIADO

Estado: FALHOU

```
{
  "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: RUNNING

```
{
  "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: CONCLUÍDO

```
{
  "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: CRIADO

```
{
  "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 ponto de recuperação

Veja a seguir exemplos de eventos.

State

- Estado: CONCLUÍDO
- Estado: EXCLUÍDO
- Estado: MODIFICADO

Estado: CONCLUÍDO


```
{
    "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: EXCLUÍDO

```
{
  "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 configurações de região

O comando a seguir é um exemplo de evento.

```
{
  "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"
  }
}
```

Eventos do Restore Job

Veja a seguir exemplos de eventos.

State

- Estado: FALHOU
- Estado: RUNNING

- Estado: CONCLUÍDO
- Estado: PENDENTE
- Estado: CRIADO

Estado: FALHOU

```
{
  "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: RUNNING

```
{
  "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: CONCLUÍDO

```
{
  "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: PENDENTE

```
{
  "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: CRIADO

```
{
  "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 com a Amazon CloudWatch

Tópicos

- CloudWatch Painel
- Métricas com CloudWatch

CloudWatch Painel

> **Note**
>
> O painel do console depende de qual região está acessando o console. Consulte Disponibilidade de recursos por Região da AWS para conferir quais regiões têm acesso ao painel de trabalhos. As regiões não listadas poderão acessar o CloudWatch painel.

Seu AWS Backup console inclui um painel para ver métricas sobre trabalhos de backup, cópia e restauração concluídos ou com falha. Nesse painel, você pode visualizar o status do trabalho por período, personalizado de acordo com o período desejado.

COMO ACESSAR O PAINEL

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. Selecione Painel no painel de navegação à esquerda.

VISUALIZAR E ENTENDER O PAINEL

O CloudWatch painel exibe vários widgets. Cada widget mostra métricas de trabalho por contagem. Cada widget mostra vários gráficos de linhas. Cada linha corresponde a um recurso protegido (se um recurso esperado não for exibido, verifique se o recurso está ativado nas Configurações). As telas não mostram trabalhos em andamento.

O eixo y (valores verticais) mostra a contagem. O eixo x (valores horizontais) mostra pontos no tempo. Se não houver pontos de dados para visualizar no status do trabalho selecionado, o valor será definido como 0 com uma linha horizontal no eixo x. A legenda que mostra os recursos ainda estará visível.

As métricas exibem informações específicas da conta e da região relacionadas ao login atual. Para ver outras contas ou regiões, você deve fazer login na conta escolhida.

PERSONALIZAR O PAINEL

Por padrão, o período exibido é de uma semana. No menu superior, há opções para redefinir o período exibido. Você pode escolher entre 1 hora, 3 horas, 12 horas, 1 dia, 3 dias e 1 semana. Além disso, você pode selecionar Personalizar para especificar um valor diferente. A personalização alterará temporariamente a visualização atual de acordo com suas especificações.

Você pode passar o mouse sobre um widget, que exibirá um botão Ampliar no canto superior direito do widget. Clique em Ampliar para abrir o widget em tela cheia. Em tela cheia, há mais opções para personalizar a exibição do gráfico, como alterar o período (o tempo entre cada ponto de dados). Quaisquer alterações não serão retidas depois que a exibição em tela cheia for fechada.

Para visualizar somente um tipo de recurso por vez, clique no texto do rótulo do tipo de recurso que você deseja visualizar na legenda do gráfico. Isso desmarcará todos os tipos de recursos. Para reverter isso, clique na caixa de cores do tipo de recurso na legenda. Para voltar à exibição padrão de todos os tipos de recursos com todos os rótulos selecionados, clique novamente no texto do rótulo de qualquer tipo de recurso selecionado.

Clicar nos três pontos verticais no canto superior direito de um widget abre um menu suspenso com opções para atualizar, ampliar, visualizar em métricas e visualizar em logs. “Exibir em métricas” abre

a métrica usada no widget no CloudWatch console. Você pode fazer qualquer alteração no widget lá e adicionar o widget a um painel personalizado no CloudWatch painel. Quaisquer alterações feitas no CloudWatch painel não serão refletidas no painel no AWS Backup Console. “Exibir como registros” abre a página de visualização de registros no CloudWatch console.

Para adicionar widgets exibidos ao seu próprio CloudWatch painel personalizado, clique no botão Adicionar ao painel localizado no canto superior direito do painel. Isso abrirá o CloudWatch console onde você poderá selecionar em qual painel personalizado adicionar todos os seis widgets.

Para obter mais informações, consulte Usando CloudWatch métricas da Amazon.

Métricas com CloudWatch

Você pode usar CloudWatch para monitorar AWS Backup métricas. O `AWS/Backup` namespace permite que você acompanhe as seguintes métricas. AWS Backup emite métricas atualizadas a CloudWatch cada 5 minutos.

O objetivo desta página de documentação é fornecer a você os materiais de referência a CloudWatch serem usados no monitoramento AWS Backup. Para saber como monitorar uma métrica usando CloudWatch, consulte o blog Amazon CloudWatch Events and Metrics for AWS Backup or Focus on Metrics and Alarms in a Single AWS Service no Guia do CloudWatch usuário. Para definir alarmes, consulte Usando CloudWatch alarmes da Amazon no Guia do CloudWatch usuário.

Categoria	Métricas	Exemplo de dimensões	Exemplo de caso de uso
Tarefas	Número de trabalhos de backup, restauração e cópia em cada estado, incluindo `CREATED`, `PENDING`, `RUNNING`, `ABORTED`, `COMPLETED` , `FAILED` e `EXPIRED`. Diferentes tipos de trabalho têm diferentes estados disponíveis.	Tipo de recurso, nome do cofre. O nome do cofre dos trabalhos de cópia é o do cofre de destino.	Monitore o número de tarefas de backup com falha em um ou mais cofres de backup específicos. Quando houver mais de cinco trabalhos com falha em uma hora, envie um e-mail ou SMS usando o Amazon SNS ou abra um tíquete para

Categoria	Métricas	Exemplo de dimensões	Exemplo de caso de uso
			a equipe de engenharia investigar. Critérios de relatório: há um valor diferente de zero
Pontos de recuperação	Número de pontos de recuperação frios e quentes em cada estado: `MODIFIED`, `COMPLETED` , `PARTIAL`, `EXPIRED`, `DELETED`.	Tipo de recurso, nome do cofre.	Rastreie o número de pontos de recuperação excluídos dos seus volumes do Amazon EBS e, separadamente, rastreie o número de pontos de recuperação quentes e frios em cada cofre de backup. Critérios de relatório: há um valor diferente de zero

> **Note**
>
> O status do trabalho de `Completed with issues` é específico somente para o AWS Backup console; ele não pode ser rastreado por meio do CloudWatch.

As tabelas a seguir listam métricas disponíveis para você.

Métrica	Descrição
`NumberOfBackupJobsCreated`	O número de trabalhos de backup AWS Backup criados.

Métrica	Descrição
`NumberOfBackupJobsPending`	O número de tarefas de backup prestes a serem executadas no AWS Backup.
`NumberOfBackupJobsRunning`	O número de trabalhos de backup em execução no momento AWS Backup.
`NumberOfBackupJobsAborted`	O número de trabalhos de backup cancelados pelo usuário.
`NumberOfBackupJobsCompleted`	O número de trabalhos de backup AWS Backup concluídos.
`NumberOfBackupJobsFailed`	O número de trabalhos de backup com status de `Failed`. Geralmente causado pelo agendamento de um trabalho de backup durante ou 1 hora antes de um recurso de banco de dados ou 4 horas antes ou durante uma janela de manutenção ou janela de backup automatizado do Amazon FSx e pela falta de AWS Backup uso para realizar backup point-in-time contínuo para restaurações. Consulte Point-in-Time Recovery para obter uma lista de serviços suportados e instruçõe s sobre como usar AWS Backup para fazer backups contínuos ou reagendar suas tarefas de backup.
`NumberOfBackupJobsExpired`	O número de tarefas de backup que têm um status de`EXPIRED`. Uma tarefa de backup muda de status `CREATED` para `EXPIRED` se um backup não puder ser iniciado dentro do horário da janela inicial.

Métrica	Descrição
NumberOfCopyJobsCreated	O número de trabalhos de cópia entre contas e entre regiões que o AWS Backup criou.
NumberOfCopyJobsRunning	O número de trabalhos de cópia entre contas e entre regiões em execução no AWS Backup.
NumberOfCopyJobsCompleted	O número de trabalhos de cópia entre contas e entre regiões que o AWS Backup concluiu.
NumberOfCopyJobsFailed	O número de trabalhos de cópia entre contas e regiões que AWS Backup tentaram, mas não puderam ser concluídos.
NumberOfRestoreJobsPending	O número de trabalhos de restauração prestes a serem executados no AWS Backup.
NumberOfRestoreJobsRunning	O número de trabalhos de restauração em execução no momento AWS Backup.
NumberOfRestoreJobsCompleted	O número de trabalhos de restauração AWS Backup concluídos.
NumberOfRestoreJobsFailed	O número de trabalhos de restauração que AWS Backup tentaram, mas não puderam ser concluídos.
NumberOfRecoveryPointsCompleted	O número de pontos de recuperação AWS Backup criados.
NumberOfRecoveryPointsPartial	O número de pontos de recuperação que AWS Backup começaram a ser criados, mas não puderam ser concluídos. AWS repete o processo posteriormente, mas como a nova tentativa ocorre posteriormente, ela retém o ponto de recuperação parcial.

Métrica	Descrição
`NumberOfRecoveryPointsExpired`	O número de pontos de recuperação que AWS Backup tentaram excluir com base no seu ciclo de vida de retenção de backup, mas não puderam ser excluídos. Você é cobrado pelo armazenamento que os backups expirados consomem e deve excluí-los manualmente.
`NumberOfRecoveryPointsDeleting`	O número de pontos de recuperação que estão AWS Backup sendo excluídos.
`NumberOfRecoveryPointsCold`	O número de pontos de recuperação AWS Backup vinculados ao armazenamento refrigerado.

Mais dimensões estão disponíveis além das listadas na tabela. Para visualizar todas as dimensões de uma métrica, digite o nome dessa métrica no `AWS/Backup` namespace da seção Métricas do CloudWatch console.

Registrando chamadas de AWS Backup API com CloudTrail

AWS Backup é integrado a AWS CloudTrailum serviço que fornece um registro das ações realizadas por um usuário, função ou AWS service (Serviço da AWS) serviço. CloudTrail captura todas as chamadas de API AWS Backup como eventos. As chamadas capturadas incluem chamadas do AWS Backup console e chamadas de código para as operações AWS Backup da API. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS Backup, o endereço IP do qual a solicitação foi feita, quando foi feita e detalhes adicionais.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita em nome de um usuário do Centro de Identidade do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

CloudTrail está ativo Conta da AWS quando você cria a conta e você tem acesso automático ao histórico de CloudTrail eventos. O histórico de CloudTrail eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento registrados em um. Região da AWS Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário. Não há CloudTrail cobrança pela visualização do histórico de eventos.

Para um registro contínuo dos eventos dos Conta da AWS últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrailLake.

CloudTrail trilhas

Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Todas as trilhas criadas usando o AWS Management Console são multirregionais. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. É recomendável criar uma trilha multirregional porque você captura todas as atividades Regiões da AWS em sua conta. Se você criar uma trilha de região única, poderá visualizar somente os eventos registrados na Região da AWS da trilha. Para obter mais informações sobre trilhas, consulte Criar uma trilha para a Conta da AWS e Criar uma trilha para uma organização no Guia do usuário do AWS CloudTrail .

Você pode entregar uma cópia dos seus eventos de gerenciamento contínuos para o bucket do Amazon S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços. Para receber informações sobre a definição de preço do Amazon S3, consulte Definição de preço do Amazon S3.

CloudTrail Armazenamentos de dados de eventos em Lake

CloudTrail O Lake permite que você execute consultas baseadas em SQL em seus eventos. CloudTrail O Lake converte eventos existentes no formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Os seletores que você aplica a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para você consultar. Para obter mais informações sobre o CloudTrail Lake, consulte Trabalhando com o AWS CloudTrail Lake no Guia AWS CloudTrail do Usuário.

CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem em custos. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja

usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

AWS Backup eventos em CloudTrail

AWS Backup gera esses CloudTrail eventos ao realizar backups, restaurações, cópias ou notificações. Esses eventos não são necessariamente gerados pelo uso das APIs AWS Backup públicas. Para obter mais informações, consulte AWS service (Serviço da AWS) os eventos no Guia AWS CloudTrail do usuário.

- `BackupDeleted`
- `BackupJobCompleted`
- `BackupJobStarted`
- `BackupSelectionDeletedDueToSLRDeletion`
- `BackupTransitionedToCold`
- `CopyJobCompleted`
- `CopyJobStarted`
- `ReportJobCompleted`
- `ReportJobStarted`
- `RestoreCompleted`
- `RestoreStarted`
- `PutBackupVaultNotifications`

Entendendo as entradas do arquivo de AWS Backup log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra as `DeleteRecoveryPoint` ações `StartBackupJobStartRestoreJob`,, e e também o `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"
    }
}
```


Registrar em log eventos de gerenciamento entre contas

Com AWS Backup, você pode gerenciar seus backups em toda Contas da AWS a sua AWS Organizationsestrutura. AWS Backup gera esses CloudTrail eventos quando você cria, atualiza ou exclui uma política de AWS Organizations backup (que aplica planos de backup às suas contas membros) ou quando há um plano de backup organizacional inválido:

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationalBackupPlan`

Exemplo: entradas de arquivos de AWS Backup log para gerenciamento de várias contas

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateOrganizationalBackupPlan` ação.


```
{
    "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"
    }
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `DeleteOrganizationalBackupPlan` ação.

```
{
    "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"
    }
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra o eventoInvalidOrganizationBackupPlan, que é enviado quando AWS Backup recebe um plano de backup inválido da 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"
}
```

Opções de notificação com AWS Backup

Há duas maneiras de receber notificações sobre AWS Backup:

- AWS As notificações do usuário podem enviar notificações, incluindo CloudWatch alarmes da Amazon e notificações de outros serviços. AWS Support
- O Amazon Simple Notification Service pode notificá-lo sobre AWS Backup eventos.

AWS Notificações do usuário e AWS Backup

AWS Backup suporta o gerenciamento de suas notificações de backup no console de notificações AWS do usuário. Com as Notificações ao usuário da AWS, você pode ver o progresso de seus trabalhos de backup, cópia e restauração e as alterações em suas políticas de backup, cofres, pontos de recuperação e configurações na Central de notificações ao usuário.

Amazon CloudWatch, EventBridge alarmes da Amazon e atualizações de AWS Support casos estão entre outros tipos de notificações que você pode gerenciar no console. Além disso, você pode configurar várias opções de entrega, incluindo e-mail, AWS Chatbot notificações e notificações AWS Console Mobile Application push.

Amazon SNS e eventos AWS Backup

AWS Backup aproveita as notificações robustas fornecidas pelo Amazon Simple Notification Service (Amazon SNS). Você pode configurar o Amazon SNS para notificá-lo sobre AWS Backup eventos no console do Amazon SNS.

Limitações

- Embora o serviço Amazon SNS permita notificações entre contas, atualmente AWS Backup não oferece suporte a esse recurso. Você deve especificar seu próprio ID de AWS conta e o ARN do recurso do seu tópico.
- AWS Backup oferece suporte a tópicos padrão para a melhor desduplicação do SNS, mas atualmente AWS Backup não oferece suporte aos tópicos FIFO do SNS para desduplicação estrita.

Casos de uso comuns

- Configure notificações para trabalhos de backup com falha seguindo as etapas em Como posso receber notificações de AWS Backup trabalhos que falharam? do AWS Premium Support.
- Analise exemplos de JSONs de notificação do Amazon SNS para trabalhos de backup concluídos, com falha e expirados na tabela de exemplos de eventos abaixo.

Para obter informações gerais sobre como criar um tópico do Amazon SNS, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

AWS Backup APIs de notificação

Depois de criar seus tópicos usando o console do Amazon SNS ou AWS Command Line Interface (AWS CLI), você pode usar as seguintes operações de AWS Backup API para gerenciar suas notificações de backup.

- DeleteBackupVaultNotifications: exclui notificações de eventos para o cofre de backup especificado.
- GetBackupVaultNotifications: lista as notificações de eventos para o cofre de backup especificado.
- PutBackupVaultNotifications: ativa as notificações para o tópico e os eventos especificados.

AWS Backup suporta os seguintes eventos:

Tipo de trabalho	Evento
Trabalho de backup	`BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED` | `CONTINUOUS_BACKUP_INTERRUPTED`
Trabalho de cópia	`COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED`
Trabalho de restauração	`RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED`
Ponto de recuperação	`RECOVERY_POINT_MODIFIED`

AWS Backup para S3 suporta dois eventos adicionais:

- O `S3_BACKUP_OBJECT_FAILED` notifica você sobre qualquer objeto do S3 que o AWS Backup não conseguiu fazer o backup durante um trabalho de backup.
- O `S3_RESTORE_OBJECT_FAILED` notifica você sobre qualquer objeto do S3 que o AWS Backup não conseguiu restaurar durante um trabalho de restauração.

Exemplos de eventos

Example Exemplo: tarefa de backup concluída

```
{
    "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 Exemplo: falha na tarefa 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 Exemplo: A tarefa de backup não pôde ser concluída durante a janela 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 exemplos de comandos de notificação

Você pode usar AWS CLI comandos para assinar, listar e excluir notificações do Amazon SNS para seus AWS Backup eventos.

Exemplo de colocação de notificação em cofre de backup

O comando a seguir faz a inscrição em um tópico do Amazon SNS para o cofre de backup especificado que notifica quando um trabalho de restauração é iniciado ou concluído, ou quando um ponto de recuperação é modificado.

```
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
```

Exemplo de obtenção de notificação de cofre de backup

O comando a seguir lista todos os eventos que têm atualmente inscrições em um tópico do Amazon SNS para o cofre de backup especificado.

```
aws backup get-backup-vault-notifications
    --backup-vault-name myVault
```

O exemplo de resultado é o seguinte:

```
{
    "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"
}
```

Exemplo de exclusão de notificação de cofre de backup

O comando a seguir anula a inscrição em um tópico do Amazon SNS para o cofre de backup especificado.

```
aws backup delete-backup-vault-notifications
    --backup-vault-name myVault
```

Especificando AWS Backup como principal de serviço

> **Note**
>
> Para permitir AWS Backup a publicação de tópicos do SNS em seu nome, você deve especificar AWS Backup como principal de serviço.

Inclua o seguinte JSON na política de acesso do tópico do Amazon SNS que você usa para AWS Backup rastrear eventos. É necessário especificar o nome de recurso da Amazon (ARN) do seu tópico.

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Para obter mais informações sobre a especificação de um principal de serviço em uma política de acesso do Amazon SNS, consulte Permitir que AWS qualquer recurso publique em um tópico no Guia do desenvolvedor do Amazon Simple Notification Service.

> **Note**
>
> Se seu tópico estiver criptografado, você deverá incluir permissões adicionais em sua política AWS Backup para permitir a publicação nele. Para obter mais informações sobre como habilitar serviços para publicar em tópicos criptografados, consulte Habilitar compatibilidade entre fontes de eventos de AWS serviços e tópicos criptografados no Guia do desenvolvedor do Amazon Simple Notification Service.

Solução de problemas AWS Backup

Ao usar AWS Backup, você pode encontrar problemas. As seções a seguir podem ajudar a solucionar alguns problemas comuns que podem ocorrer.

Para perguntas gerais sobre AWS Backup, consulte as AWS Backup perguntas frequentes. Você também pode procurar respostas e postar dúvidas no Fórum do AWS Backup.

Tópicos

Solução de problemas gerais

Ao fazer backup e restaurar recursos, você deve ter permissão para usar AWS Backup e acessar os recursos que deseja proteger. A maneira mais fácil de ter as permissões adequadas é escolher a função padrão ao atribuir recursos a um plano de backup. Para obter mais informações sobre o controle de acesso usando AWS Identity and Access Management (IAM) com AWS Backup, consulteControle de acesso.

Se você receber um `AccessDenied` erro ao tentar acessar um AWS Backup recurso, como um cofre de backup, o recurso não existe ou você não tem permissões para acessá-lo.

Se tiver problemas com o backup e a restauração de um determinado tipo de recurso, pode ser útil revisar o tópico de solução de problemas para esse recurso. Para obter mais informações, consulte os links em Como AWS Backup funciona com AWS os serviços suportados.

Se você AWS Backup não conseguir criar ou excluir um recurso, saiba mais sobre o problema usando AWS CloudTrail para visualizar mensagens de erro ou registros. Para obter mais informações sobre como usar CloudTrail com AWS Backup, consulteRegistrando chamadas de AWS Backup API com CloudTrail.

Solução de problemas de criação de recursos

As informações a seguir podem ajudá-lo a solucionar problemas ao criar backups.

- Em geral, os serviços de banco de dados da AWS não podem iniciar os backups uma hora antes ou durante a janela de manutenção ou a janela de backup automático. O Amazon FSx não pode iniciar backups quatro horas antes ou durante a janela de manutenção ou a janela de backup automático (o Amazon Aurora está isento dessa restrição de janela de manutenção). Haverá falha nos backups de snapshot programados durante esses horários. Uma exceção: quando você opta AWS Backup por usar backups instantâneos e contínuos de um serviço compatível, não precisa mais se preocupar com essas janelas, pois elas AWS Backup serão agendadas para você. Consulte Point-in-Time Recovery para obter uma lista de serviços suportados e instruções sobre como usar AWS Backup para fazer backups contínuos.
- Haverá falha na criação de backups para tabelas do DynamoDB enquanto as tabelas estiverem sendo criadas. Normalmente, criar uma tabela do DynamoDB leva alguns minutos.
- O backup de sistemas de arquivos do Amazon EFS pode levar até sete dias quando os sistemas de arquivos são muito grandes. É possível colocar somente um backup simultâneo de cada vez na fila para um sistema de arquivos do Amazon EFS. Se um backup subsequente for colocado na fila enquanto um anterior ainda estiver em andamento, a janela de backup poderá expirar e nenhum backup será criado.
- O Amazon EBS tem uma cota flexível de 100.000 backups Região da AWS por conta, e backups adicionais falham quando essa cota é atingida. Se você atingir essa cota, poderá excluir backups em excesso ou solicitar um aumento de limite. Para obter mais informações sobre como solicitar um aumento de cota, consulte Cotas de serviço da AWS.
- Ao criar backups do Amazon Relational Database Service (RDS), considere o seguinte:
  - Se você não usar AWS Backup para gerenciar tanto os snapshots do Amazon RDS quanto os backups contínuos com point-in-time recuperação, seus backups falharão se iniciados se forem programados ou feitos sob demanda durante a janela de backup diário de 30 minutos configurável pelo usuário. Para obter mais informações sobre backups automatizados do Amazon RDS, consulte Trabalhar com backups no Guia do usuário do Amazon RDS. Você pode evitar essa limitação usando AWS Backup para gerenciar tanto os snapshots do Amazon RDS quanto os backups contínuos com point-in-time recuperação.
  - Se você iniciar um trabalho de backup no console do Amazon RDS, isso poderá entrar em conflito com um trabalho de backup de clusters do Aurora, causando o erro `Backup job expired before completion.`. Se isso ocorrer, configure uma janela de backup mais longa no AWS Backup.

- AWS Backup atualmente não transmite o grupo de opções do TDE quando um trabalho de cópia é criado. Se pretender usar esse grupo de opções para criar trabalhos de cópia, você deverá usar o console do Amazon RDS ou a API do Amazon RDS em vez de ferramentas do AWS Backup . Consulte Copiar um grupo de opções no Guia do usuário do Amazon Relational Database Service para obter mais informações.
- ERRO: os backups sob demanda são concluídos, mas haverá falha nos backups programados com o erro “A chave do KMS do snapshot de origem não existe, não está habilitada ou você não tem permissões para acessá-la”. O trabalho sob demanda é concluído porque usa a chamada de API `CopyDBSnapshot`, que não exige acesso ao KMS.

  SOLUÇÃO: adicione o perfil do IAM à sua chave do KMS. Isso pode ser feito permitindo o perfil em sua política de chaves do KMS.

  Para editar aa política,

  1. Abra o console do KMS.
  2. Selecione Chaves gerenciadas pelo cliente na barra de navegação esquerda.
  3. Clique na chave gerenciada pelo cliente que deseja editar.
  4. Em Política de chave, clique em Alternar para visualização de política.
  5. Clique em Edit.
  6. Adicione o perfil.

Solução de problemas de exclusão de recursos

Os pontos de recuperação criados por AWS Backup não podem ser excluídos na janela do console do recurso protegido. Você pode excluí-los no AWS Backup console selecionando-os no cofre em que estão armazenados e, em seguida, escolhendo Excluir.

Para excluir um ponto de recuperação ou um cofre de backup, você precisa das permissões apropriadas. Para obter mais informações sobre o controle de acesso usando o IAM com AWS Backup, consulteControle de acesso.

Solução de problemas de recursos de restauração

Restaurar usando a API

Para restaurar um backup de forma programática, use a operação StartRestoreJob da API.

Para obter os metadados de configuração com os quais seu backup foi criado, é possível chamar GetRecoveryPointRestoreMetadata.

Consulte Restaurar um backup para obter mais informações.

Restaurar um backup usando o console

- Restaurar dados do Amazon S3
- Restaurar uma máquina virtual
- Restaurar um sistema de arquivos do Amazon FSx
- Restaurar um volume do Amazon EBS
- Restaurar um sistema de arquivos do Amazon EFS
- Restaurar uma tabela do Amazon DynamoDB
- Restaurar um banco de dados do RDS
- Restaurar um cluster do Aurora
- Restaurar uma instância do Amazon EC2
- Restaurar um volume do Storage Gateway
- Restaure um cluster do Amazon DocumentDB
- Restaurar um cluster do Neptune

Solução de problemas de formatação

Quando um caractere curinga (*) é incluído para o valor em um parâmetro, o curinga é processado para incluir valores que não sejam espaços em branco. Os valores em um par de valores-chave que contêm espaços em branco não serão incluídos como parte do curinga.

API do AWS Backup

Além de usar o console, você pode usar a API do AWS Backup para configurar e gerenciar o AWS Backup e seus recursos de forma programática. Esta seção descreve ações e tipos de dados do AWS Backup. Ele contém a referência da API para o AWS Backup.

API do AWS Backup

- Ações do AWS Backup
- Tipos de dados do AWS Backup

Ações

As seguintes ações são compatíveis com o AWS Backup:

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework
- DeleteRecoveryPoint

- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection
- GetSupportedResourceTypes

- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob
- StartCopyJob

- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

As ações a seguir são compatíveis com o AWS Backup gateway:

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines

- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AWS Backup

As ações a seguir são compatíveis com o AWS Backup:

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework

- DeleteRecoveryPoint
- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection

- GetSupportedResourceTypes
- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob

- StartCopyJob
- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

CancelLegalHold

Serviço: AWS Backup

Remove a retenção legal especificada em um ponto de recuperação. Essa ação só pode ser executada por um usuário com permissões suficientes.

Sintaxe da Solicitação

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

CancelDescription

Uma string que descreve o motivo da remoção da retenção legal.

Obrigatório: Sim

legalHoldId

O ID da retenção legal.

Obrigatório: Sim

RetainRecordInDays

O valor inteiro, em dias, após o qual remover a retenção legal.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 201
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 201 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidResourceStateException

AWS Backup já está executando uma ação nesse ponto de recuperação. Ele não pode realizar a ação solicitada até que a primeira ação seja concluída. Tente novamente mais tarde.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Cria um plano de backup usando o nome do plano de backup e as regras de backup. Um plano de backup é um documento que contém informações AWS Backup usadas para agendar tarefas que criam pontos de recuperação para recursos.

Se chamar `CreateBackupPlan` com um plano existente, você receberá uma exceção `AlreadyExistsException`.

Sintaxe da Solicitação

```
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"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

BackupPlan

O corpo de um plano alternativo. Inclui um `BackupPlanName` e um ou mais conjuntos de `Rules`.

Tipo: objeto BackupPlanInput

Obrigatório: Sim

BackupPlanTags

As tags a serem atribuídas ao plano de backup.

Tipo: mapa de string para string

Obrigatório: não

CreatorRequestId

Identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Se a solicitação incluir um `CreatorRequestId` que corresponda a um plano de backup existente, esse plano será retornado. Esse parâmetro é opcional.

Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AdvancedBackupSettings

As configurações de um tipo de recurso. Essa opção só está disponível para trabalhos de backup do Serviço de Cópias de Sombra de Volume (VSS) do Windows.

Tipo: matriz de objetos AdvancedBackupSetting

BackupPlanArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um plano de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: sequência

BackupPlanId

O ID do plano de backup.

Tipo: sequência

CreationDate

A data e hora em que o plano de backup foi criado, em formato de hora Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

VersionId

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. Eles não podem ser editados.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AlreadyExistsException

O recurso necessário já existe.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Cria um documento JSON que especifica um conjunto de recursos a serem atribuídos a um plano de backup. Para ver exemplos, consulte Atribuir recursos de forma programática.

Sintaxe da Solicitação

```
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"
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupPlanId

O ID do plano de backup.

Obrigatório: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

BackupSelection

O corpo de uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Tipo: objeto BackupSelection

Obrigatório: Sim

CreatorRequestId

Uma string exclusiva que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Esse parâmetro é opcional.

Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupPlanId

O ID do plano de backup.

Tipo: sequência

CreationDate

A data e hora em que uma seleção de backup é criada, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

SelectionId

Identifica exclusivamente o corpo de uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AlreadyExistsException

O recurso necessário já existe.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Cria um contêiner lógico onde os backups são armazenados. Uma solicitação `CreateBackupVault` inclui um nome, opcionalmente uma ou mais tags de recurso, uma chave de criptografia e um ID de solicitação.

> **Note**
>
> Não inclua dados confidenciais, como números de passaporte, no nome de um cofre de backup.

Sintaxe da Solicitação

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados. Eles consistem em letras, números e hifens.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

BackupVaultTags

As tags a serem atribuídas ao cofre de backup.

Tipo: mapa de string para string

Obrigatório: não

CreatorRequestId

Uma string exclusiva que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Esse parâmetro é opcional.

Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

EncryptionKeyArn

A chave de criptografia no lado do servidor usada para proteger seus backups, por exemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: sequência

Obrigatório: não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupVaultArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da em que são criados. Eles consistem em letras minúsculas, números e hifens.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

A data e hora em que um cofre de backup foi criado, em formato de hora Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AlreadyExistsException

O recurso necessário já existe.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Cria uma framework com um ou mais controles. Uma framework é uma coleção de controles podem ser utilizados para avaliar suas práticas de backup. Usando controles personalizáveis pré-criados para definir suas políticas, você pode avaliar se as suas práticas de backup estão em conformidade com as suas políticas e quais recursos ainda não estão em conformidade.

Sintaxe da Solicitação

```
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"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

FrameworkControls

Os controles que compõem a estrutura. Cada controle na lista tem um nome, parâmetros de entrada e escopo.

Tipo: matriz de objetos FrameworkControl

Obrigatório: Sim

FrameworkDescription

Uma descrição opcional da framework com no máximo 1.024 caracteres.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 1.024.

Padrão: `.*\S.*`

Obrigatório: não

FrameworkName

O nome exclusivo da framework. Esse nome deve ter entre 1 e 256 caracteres, começando com uma letra, e consistir em letras (a-z, A-Z), números (0-9) e sublinhados (_).

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Exigido: Sim

FrameworkTags

As tags a serem atribuídas à estrutura.

Tipo: mapa de string para string

Obrigatório: não

IdempotencyToken

Uma string escolhida pelo cliente que você pode usar para distinguir entre chamadas idênticas para `CreateFrameworkInput`. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

FrameworkArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

FrameworkName

O nome exclusivo da framework. Esse nome deve ter entre 1 e 256 caracteres, começando com uma letra, e consistir em letras (a-z, A-Z), números (0-9) e sublinhados (_).

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AlreadyExistsException

O recurso necessário já existe.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Cria uma retenção legal em um ponto de recuperação (backup). Uma retenção legal é uma restrição à alteração ou exclusão de um backup até que um usuário autorizado cancele a retenção legal. haverá falha em qualquer ação para excluir ou desassociar um ponto de recuperação com um erro se uma ou mais retenções legais ativas estiverem no ponto de recuperação.

Sintaxe da Solicitação

```
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"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

Description

A descrição da retenção legal.

Tipo: string

Obrigatório: Sim

IdempotencyToken

Essa é uma string escolhida pelo usuário usada para distinguir entre chamadas idênticas. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

RecoveryPointSelection

Os critérios para atribuir um conjunto de recursos, como tipos de recursos ou cofres de backup.

Tipo: objeto RecoveryPointSelection

Obrigatório: Não

Tags

Tags opcionais a serem incluídas. Uma tag é um par de chave/valor que ajuda você a gerenciar, filtrar e pesquisar seus recursos. Os caracteres permitidos incluem letras, números e espaços em UTF-8, além dos seguintes caracteres especiais: + - = . _ : /.

Tipo: mapa de string para string

Obrigatório: não

Title

O título da retenção legal.

Tipo: string

Obrigatório: Sim

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationDate

A hora em que a retenção legal foi criada.

Tipo: carimbo de data/hora

Description

A descrição da retenção legal.

Tipo: sequência

LegalHoldArn

O nome de recurso da Amazon (ARN) da retenção legal.

Tipo: sequência

LegalHoldId

O ID da retenção legal.

Tipo: sequência

RecoveryPointSelection

Os critérios a serem atribuídos a um conjunto de recursos, como tipos de recursos ou cofres de backup.

Tipo: objeto RecoveryPointSelection

Status

O status da retenção legal.

Tipo: sequências

Valores Válidos: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

O título da retenção legal.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Cria um contêiner lógico para o qual os backups podem ser copiados.

Essa solicitação inclui um nome, a região, o número máximo de dias de retenção, o número mínimo de dias de retenção e, opcionalmente, pode incluir tags e um ID de solicitação do criador.

> **Note**
>
> Não inclua dados confidenciais, como números de passaporte, no nome de um cofre de backup.

Sintaxe da Solicitação

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup logicamente isolados são identificados por nomes que são exclusivos da conta usada para criá-los e a região em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

BackupVaultTags

As etiquetas a serem atribuídas ao cofre.

Tipo: mapa de string para string

Obrigatório: não

CreatorRequestId

O ID da solicitação de criação.

Esse parâmetro é opcional. Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

MaxRetentionDays

O período máximo de retenção durante o qual o cofre retém seus pontos de recuperação. Se esse parâmetro não estiver especificado, o AWS Backup não aplicará um período máximo de retenção nos pontos de recuperação no cofre (permitindo armazenamento indefinido).

Se esse parâmetro for especificado, qualquer trabalho de backup ou cópia para o cofre deverá ter uma política de ciclo de vida com um período de retenção igual ou inferior ao período máximo de retenção. Se o período de retenção do trabalho for maior do que o período máximo de retenção, haverá falha do cofre no trabalho de backup ou de cópia e você deverá modificar as configurações do ciclo de vida ou usar um cofre diferente.

Tipo: longo

Obrigatório: Sim

MinRetentionDays

Essa configuração especifica o período mínimo de retenção que o cofre retém seus pontos de recuperação. Se esse parâmetro não for especificado, o período mínimo de retenção será aplicado.

Se for especificado, qualquer trabalho de backup ou de cópia para o cofre deverá ter uma política de ciclo de vida com um período de retenção igual ou superior ao período mínimo de retenção. Se o período de retenção do trabalho for mais curto do que o período mínimo de retenção, haverá falha do cofre no trabalho de backup ou de cópia e você deverá modificar as configurações do ciclo de vida ou usar um cofre diferente.

Tipo: longo

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupVaultArn

O ARN (Amazon Resource Name) do cofre.

Tipo: sequência

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup logicamente isolados são identificados por nomes que são exclusivos da conta usada para criá-los e a região em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

A data e a hora em que o cofre foi criado.

Esse valor está no formato Unix, Tempo Universal Coordenado (UTC) e tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

VaultState

O estado atual do cofre.

Tipo: sequências

Valores Válidos: `CREATING | AVAILABLE | FAILED`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AlreadyExistsException

O recurso necessário já existe.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Cria um plano de relatório. Um plano de relatório é um documento que contém informações sobre o conteúdo do relatório e onde AWS Backup será entregue.

Se chamar `CreateReportPlan` com um plano existente, você receberá uma exceção `AlreadyExistsException`.

Sintaxe da Solicitação

```
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"
   }
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

IdempotencyToken

Uma string escolhida pelo cliente que pode ser usada para distinguir entre chamadas idênticas para `CreateReportPlanInput`. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

ReportDeliveryChannel

Uma estrutura que contém informações sobre onde e como entregar seus relatórios, especificamente o nome do bucket do Amazon S3, o prefixo de chave do S3 e os formatos dos relatórios.

Tipo: objeto ReportDeliveryChannel

Obrigatório: Sim

ReportPlanDescription

Uma descrição opcional do plano de relatório com 1.024 caracteres no máximo.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 1.024.

Padrão: `.*\S.*`

Obrigatório: não

ReportPlanName

O nome exclusivo do plano de relatório. Esse nome deve ter entre 1 e 256 caracteres, começando com uma letra, e consistir em letras (a-z, A-Z), números (0-9) e sublinhados (_).

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Exigido: Sim

ReportPlanTags

As tags a serem atribuídas ao plano de relatório.

Tipo: mapa de string para string

Obrigatório: não

ReportSetting

Identifica o modelo do relatório. Relatórios são criados utilizando um modelo de relatório. Os modelos de relatório são:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Se o modelo de relatório for `RESOURCE_COMPLIANCE_REPORT` ou`CONTROL_COMPLIANCE_REPORT`, esse recurso de API também descreve a cobertura do relatório por Regiões da AWS estruturas.

Tipo: objeto ReportSetting

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A data e hora em que o cofre de backup foi criado, em formato de hora Unix e Tempo Universal Coordenado (UTC). O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

ReportPlanArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

ReportPlanName

O nome exclusivo do plano de relatório.

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AlreadyExistsException

O recurso necessário já existe.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Cria um plano de teste de restauração.

A primeira das duas etapas para criar um plano de teste de restauração. Depois que essa solicitação for bem-sucedida, conclua o procedimento usando CreateRestoreTestingSelection.

Sintaxe da Solicitação

```
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"
   }
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

CreatorRequestId

Essa é uma string exclusiva que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Esse parâmetro é opcional. Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

RestoreTestingPlan

Um plano de testes de restauração deve conter uma string `RestoreTestingPlanName` exclusiva criada por você e deve conter um cron `ScheduleExpression`. Você também pode incluir um inteiro `StartWindowHours` e uma string `CreatorRequestId`.

`RestoreTestingPlanName` é uma string exclusiva que é o nome do plano de testes de restauração. Ele não pode ser alterado após a criação e deve consistir somente em caracteres alfanuméricos e sublinhados.

Tipo: objeto RestoreTestingPlanForCreate

Obrigatório: Sim

Tags

As tags a serem atribuídas ao plano de teste de restauração.

Tipo: mapa de string para string

Obrigatório: Não

Sintaxe da Resposta

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 201.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A data e hora em que um plano de testes de restauração foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

RestoreTestingPlanArn

Um nome do recurso da Amazon (ARN) que identifica exclusivamente o plano de testes de restauração criado.

Tipo: sequência

RestoreTestingPlanName

Essa string exclusiva é o nome do plano de testes de restauração.

O nome não poderá ser alterado após a criação. Ele só pode conter caracteres alfanuméricos e sublinhados. O tamanho máximo é 50.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AlreadyExistsException

O recurso necessário já existe.

Código de Status HTTP: 400

ConflictException

AWS Backup não pode realizar a ação que você solicitou até que termine de executar uma ação anterior. Tente novamente mais tarde.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa solicitação pode ser enviada após a CreateRestoreTestingPlan solicitação ser retornada com sucesso. Essa é a segunda parte da criação de um plano de testes de recursos e deve ser concluída sequencialmente.

Isso consiste em `RestoreTestingSelectionName`, `ProtectedResourceType` e um dos seguintes:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Cada tipo de recurso protegido pode ter um único valor.

Uma seleção de testes de restauração pode incluir um valor curinga (“*”) para `ProtectedResourceArns` com `ProtectedResourceConditions`. Como alternativa, você pode incluir até 30 ARNs de recursos protegidos específicos em `ProtectedResourceArns`.

Não é possível selecionar por tipos de recursos protegidos e ARNs específicos. A solicitação falhará se ambos forem incluídos.

Sintaxe da Solicitação

```
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
   }
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

RestoreTestingPlanName

Insira o nome do plano de teste de restauração que foi retornado da CreateRestoreTestingPlan solicitação relacionada.

Obrigatório: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

CreatorRequestId

Essa é uma string exclusiva opcional que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

RestoreTestingSelection

Isso consiste em `RestoreTestingSelectionName`, `ProtectedResourceType` e um dos seguintes:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Cada tipo de recurso protegido pode ter um único valor.

Uma seleção de testes de restauração pode incluir um valor curinga (“*”) para `ProtectedResourceArns` com `ProtectedResourceConditions`. Como alternativa, você pode incluir até 30 ARNs de recursos protegidos específicos em `ProtectedResourceArns`.

Tipo: objeto RestoreTestingSelectionForCreate

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 201.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A hora em que a seleção do teste de recursos foi criada.

Tipo: carimbo de data/hora

RestoreTestingPlanArn

O ARN do plano de teste de restauração ao qual a seleção do teste de restauração está associada.

Tipo: sequência

RestoreTestingPlanName

O nome do plano de teste de restauração.

O nome não poderá ser alterado após a criação. Ele só pode conter caracteres alfanuméricos e sublinhados. O tamanho máximo é 50.

Tipo: sequência

RestoreTestingSelectionName

O nome da seleção do teste de restauração para o plano de teste de restauração relacionado.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AlreadyExistsException

O recurso necessário já existe.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui um plano de backup. É possível excluir um plano de backup somente depois que todas as seleções de recursos associadas forem excluídas. A exclusão de um plano de backup exclui a versão atual do plano. As versões anteriores, se houver, ainda existirão.

Sintaxe da Solicitação

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupPlanId

Identifica exclusivamente um plano de backup.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupPlanArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um plano de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: sequência

BackupPlanId

Identifica exclusivamente um plano de backup.

Tipo: sequência

DeletionDate

A data e hora em que um plano de backup foi excluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `DeletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

VersionId

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. IDs de versão não podem ser editados.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui a seleção de recursos associada a um plano de backup especificado pelo `SelectionId`.

Sintaxe da Solicitação

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupPlanId

Identifica exclusivamente um plano de backup.

Obrigatório: Sim

selectionId

Identifica de forma exclusiva uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui o cofre de backup identificado por seu nome. Só será possível excluir um cofre se ele estiver vazio.

Sintaxe da Solicitação

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui o documento de política que gerencia as permissões em um cofre de backup.

Sintaxe da Solicitação

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui o AWS Backup Vault Lock de um cofre de backup especificado pelo nome de um cofre de backup.

Se a configuração do Vault Lock for imutável, não será possível excluir o Vault Lock usando operações de API e você receberá uma `InvalidRequestException` se tentar fazer isso. Para obter mais informações, consulte Vault Lock no Guia do AWS Backup desenvolvedor.

Sintaxe da Solicitação

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome do cofre de backup do qual excluir o AWS Backup Vault Lock.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui as notificações de eventos para o cofre de backup especificado.

Sintaxe da Solicitação

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui a framework especificada por um nome de framework.

Sintaxe da Solicitação

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

frameworkName

O nome exclusivo de uma framework.

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Exigido: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

AWS Backup não pode realizar a ação que você solicitou até que ela termine de executar uma ação anterior. Tente novamente mais tarde.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui o ponto de recuperação especificado por um ID de ponto de recuperação.

Se o ID do ponto de recuperação pertencer a um backup contínuo, chamar esse endpoint excluirá o backup contínuo existente e interromperá o backup contínuo futuro.

Quando as permissões de um perfil do IAM são insuficientes para chamar essa API, o serviço envia de volta uma resposta HTTP 200 com um corpo HTTP vazio, mas o ponto de recuperação não é excluído. Em vez disso, ele entra em um estado `EXPIRED`.

Os pontos de recuperação `EXPIRED` podem ser excluídos com essa API quando o perfil do IAM tiver a ação `iam:CreateServiceLinkedRole`. Para saber mais sobre como adicionar esse perfil, consulte Solucionar problemas com exclusões manuais.

Se o usuário ou perfil for excluído ou se a permissão no perfil for removida, haverá falha na exclusão e ela entrará em um estado `EXPIRED`.

Sintaxe da Solicitação

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

recoveryPointArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

InvalidResourceStateException

AWS Backup já está executando uma ação nesse ponto de recuperação. Ele não pode realizar a ação solicitada até que a primeira ação seja concluída. Tente novamente mais tarde.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui o plano de relatório especificado por um nome de plano de relatório.

Sintaxe da Solicitação

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

reportPlanName

O nome exclusivo de um plano de relatório.

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Exigido: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

AWS Backup não pode realizar a ação que você solicitou até que ela termine de executar uma ação anterior. Tente novamente mais tarde.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa solicitação exclui o plano de testes de restauração especificado.

A exclusão só ocorrerá com sucesso se todas as seleções de testes de restauração associadas forem excluídas primeiro.

Sintaxe da Solicitação

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

RestoreTestingPlanName

Nome exclusivo obrigatório do plano de testes de restauração que você deseja excluir.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 204
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 204 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Insira o nome do plano de testes de restauração e o nome da seleção de testes de restauração.

Todas as seleções de testes associadas a um plano de testes de restauração devem ser excluídas antes que o plano de testes de restauração possa ser excluído.

Sintaxe da Solicitação

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

RestoreTestingPlanName

Nome exclusivo obrigatório do plano de testes de restauração que contém a seleção de testes de restauração que você deseja excluir.

Obrigatório: Sim

RestoreTestingSelectionName

Nome exclusivo obrigatório da seleção de testes de restauração que você deseja excluir.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 204
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 204 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna os detalhes do trabalho de backup para o `BackupJobId` especificado.

Sintaxe da Solicitação

```
GET /backup-jobs/backupJobId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupJobId

Identifica de forma exclusiva uma solicitação para AWS Backup fazer backup de um recurso.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AccountId

Retorna o ID da conta que é proprietária do trabalho de backup.

Tipo: string

Padrão: `^[0-9]{12}$`

BackupJobId

Identifica de forma exclusiva uma solicitação para AWS Backup fazer backup de um recurso.

Tipo: sequência

BackupOptions

Representa as opções especificadas como parte do plano de backup ou do trabalho de backup sob demanda.

Tipo: mapa de string para string

Padrão da chave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Padrão de valor: `^[a-zA-Z0-9\-\_\.]{1,50}$`

BackupSizeInBytes

O tamanho de um backup, em bytes.

Tipo: longo

BackupType

Representa o tipo real de backup selecionado para um trabalho de backup. Por exemplo, se um backup bem-sucedido do Serviço de Cópias de Sombra de Volume (VSS) do Windows tiver sido feito, o `BackupType` retornará `"WindowsVSS"`. Se `BackupType` estiver vazio, então o tipo de backup foi um backup normal.

Tipo: sequência

BackupVaultArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

BytesTransferred

O tamanho em bytes transferido para um cofre de backup no momento em que o status do trabalho foi consultado.

Tipo: longo

ChildJobsInState

Isso retorna as estatísticas dos trabalhos de backup filho (aninhados) incluídos.

Tipo: mapa de string para string

Chaves válidas: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

CompletionDate

A data e a hora em que um trabalho de criação de backup é concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

CreatedBy

Contém informações de identificação sobre a criação de uma tarefa de backup, incluindo `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` e `BackupRuleId` do plano de backup usado para criá-lo.

Tipo: objeto RecoveryPointCreator

CreationDate

A data e hora em que o trabalho de backup foi criado, em formato de hora Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

ExpectedCompletionDate

A data e a hora em que se espera que um trabalho de backup de recursos seja concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `ExpectedCompletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

IamRoleArn

Especifica o ARN do perfil do IAM usado para criar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: sequência

InitiationDate

A data em que uma tarefa de backup foi iniciada.

Tipo: carimbo de data/hora

IsParent

Isso retorna o valor booliano de que um trabalho de backup é um trabalho pai (composto).

Tipo: booliano

MessageCategory

A contagem de tarefas para a categoria de mensagem especificada.

Exemplos de strings podem incluir `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `INVALIDPARAMETERS`. Veja Monitoramento para obter uma lista de MessageCategory sequências de caracteres aceitas.

Tipo: sequência

NumberOfChildJobs

Isso retorna o número de trabalhos de backup filho (aninhados).

Tipo: longo

ParentJobId

Isso retorna o ID do trabalho de backup do recurso pai (composto).

Tipo: sequência

PercentDone

Contém uma porcentagem estimada de conclusão de um trabalho no momento em que o status do trabalho foi consultado.

Tipo: sequência

RecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

ResourceArn

Um ARN identifica de forma exclusiva um recurso salvo. O formato do ARN depende do tipo de recurso.

Tipo: sequência

ResourceName

O nome não exclusivo do recurso que pertence ao backup especificado.

Tipo: sequência

ResourceType

O tipo de AWS recurso a ser copiado; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

Especifica a hora em formato Unix e Tempo Universal Coordenado (UTC) em que uma tarefa de backup deve ser iniciada antes que seja cancelada. O valor é calculado adicionando a janela inicial ao horário programado. Portanto, se o horário programado fosse às 18h e a janela inicial fosse 2 horas, o horário `StartBy` seria às 20h na data especificada. O valor de `StartBy` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

State

O estado atual de um trabalho de backup.

Tipo: sequências

Valores Válidos: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

Uma mensagem detalhada explicando o status do trabalho para fazer backup de um recurso.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

DependencyFailureException

Um AWS serviço ou recurso dependente retornou um erro ao AWS Backup serviço e a ação não pode ser concluída.

Código de Status HTTP: 500

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna metadados sobre um cofre de backup especificado por seu nome.

Sintaxe da Solicitação

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

BackupVaultAccountId

O ID da conta do cofre de backup especificado.

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupVaultArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da em que são criados.

Tipo: sequência

CreationDate

A data e hora em que o cofre de backup foi criado, em formato de hora Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

CreatorRequestId

Uma string exclusiva que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Esse parâmetro é opcional. Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

EncryptionKeyArn

A chave de criptografia no lado do servidor usada para proteger seus backups, por exemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: sequência

LockDate

A data e a hora em que a configuração do AWS Backup Vault Lock não pode ser alterada ou excluída.

Se tiver aplicado o Vault Lock ao seu cofre sem especificar uma data de bloqueio, você poderá alterar qualquer uma das configurações do Vault Lock ou excluir totalmente o Vault Lock do cofre, a qualquer momento.

Esse valor está no formato Unix, Tempo Universal Coordenado (UTC) e tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Locked

Um booleano que indica se o AWS Backup Vault Lock está atualmente protegendo o cofre de backup. `True`significa que o Vault Lock faz com que as operações de exclusão ou atualização nos pontos de recuperação armazenados no cofre falhem.

Tipo: booliano

MaxRetentionDays

A configuração AWS Backup Vault Lock que especifica o período máximo de retenção em que o cofre retém seus pontos de recuperação. Se esse parâmetro não for especificado, o Vault Lock não aplicará um período máximo de retenção nos pontos de recuperação no cofre (permitindo o armazenamento indefinido).

Se esse parâmetro for especificado, qualquer trabalho de backup ou de cópia para o cofre deverá ter uma política de ciclo de vida com um período de retenção igual ou inferior ao período máximo de retenção. Se o período de retenção do trabalho for maior do que o período máximo de retenção, haverá falha no trabalho de backup ou de cópia do cofre e você deverá modificar

as configurações do ciclo de vida ou usar um cofre diferente. Os pontos de recuperação já armazenados no cofre antes do Vault Lock não serão afetados.

Tipo: longo

MinRetentionDays

A configuração do AWS Backup Vault Lock que especifica o período mínimo de retenção em que o cofre retém seus pontos de recuperação. Se esse parâmetro não for especificado, o Vault Lock não aplicará um período mínimo de retenção.

Se esse parâmetro for especificado, qualquer trabalho de backup ou de cópia para o cofre deverá ter uma política de ciclo de vida com um período de retenção igual ou superior ao período mínimo de retenção. Se o período de retenção do trabalho for inferior do que o período mínimo de retenção, haverá falha do cofre no trabalho de backup ou de cópia e você deverá modificar as configurações do ciclo de vida ou usar um cofre diferente. Os pontos de recuperação já armazenados no cofre antes do Vault Lock não serão afetados.

Tipo: longo

NumberOfRecoveryPoints

O número de pontos de recuperação armazenados em um cofre de backup.

Tipo: longo

VaultType

O tipo de cofre descrito.

Tipo: sequências

Valores Válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna os metadados associados à criação de uma cópia de um recurso.

Sintaxe da Solicitação

```
GET /copy-jobs/copyJobId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

copyJobId

Identifica de forma exclusiva um trabalho de cópia.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CopyJob

Contém informações detalhadas sobre um trabalho de cópia.

Tipo: objeto CopyJob

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna os detalhes da framework para o `FrameworkName` especificado.

Sintaxe da Solicitação

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

frameworkName

O nome exclusivo de uma framework.

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Exigido: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A data e a hora em que a framework é criada, na representação ISO 8601. O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, 2020-07-10T15:00:00.000-08:00 representa o dia 10 de julho de 2020 às 15:00, 8 horas antes do UTC.

Tipo: carimbo de data/hora

DeploymentStatus

O status de implantação de uma framework. Os status são:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Tipo: sequência

FrameworkArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

FrameworkControls

Os controles que compõem a estrutura. Cada controle na lista tem um nome, parâmetros de entrada e escopo.

Tipo: matriz de objetos FrameworkControl

FrameworkDescription

Uma descrição opcional da framework.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 1.024.

Padrão: `.*\S.*`

FrameworkName

O nome exclusivo de uma framework.

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

Uma framework consiste em um ou mais controles. Cada controle rege um recurso, como planos de backup, seleções de backup, cofres de backup ou pontos de recuperação. Também é possível ativar ou desativar a gravação do AWS Config de cada recurso. Os status são:

- `ACTIVE` quando a gravação é ativada para todos os recursos controlados pela framework.
- `PARTIALLY_ACTIVE` quando a gravação é desativada para pelo menos um recurso controlado pela framework.
- `INACTIVE` quando a gravação é desativada para todos os recursos controlados pela framework.
- `UNAVAILABLE`quando AWS Backup não consegue validar o status da gravação no momento.

Tipo: sequência

IdempotencyToken

Uma string escolhida pelo cliente que pode ser usada para distinguir entre chamadas idênticas para `DescribeFrameworkOutput`. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface

- 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

Serviço: AWS Backup

Descreve se a AWS conta optou por fazer backup entre contas. Retorna um erro se a conta não for membro de uma organização do Organizations. Exemplo: `describe-global-settings --region us-west-2`

Sintaxe da Solicitação

```
GET /global-settings HTTP/1.1
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

GlobalSettings

O status do sinalizador `isCrossAccountBackupEnabled`.

Tipo: mapa de string para string

LastUpdateTime

A data e hora em que o sinalizador `isCrossAccountBackupEnabled` foi atualizado pela última vez. Essa atualização está em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastUpdateTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna informações sobre um recurso salvo, incluindo a última vez em que foi feito o backup, seu Amazon Resource Name (ARN) e o tipo de AWS serviço do recurso salvo.

Sintaxe da Solicitação

```
GET /resources/resourceArn HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

resourceArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

LastBackupTime

A data e hora em que o backup de um recurso foi feito pela última vez, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastBackupTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

LastBackupVaultArn

O ARN (Amazon Resource Name) do cofre de backup que contém o ponto de recuperação de backup mais recente.

Tipo: sequência

LastRecoveryPointArn

O ARN (Amazon Resource Name) do ponto de recuperação mais recente.

Tipo: sequência

LatestRestoreExecutionTimeMinutes

O tempo, em minutos, que o trabalho de restauração mais recente levou para ser concluído.

Tipo: longo

LatestRestoreJobCreationDate

A data de criação da tarefa de restauração mais recente.

Tipo: carimbo de data/hora

LatestRestoreRecoveryPointCreationDate

A data em que o ponto de recuperação mais recente foi criado.

Tipo: carimbo de data/hora

ResourceArn

Um ARN que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

ResourceName

O nome do recurso que pertence ao backup especificado.

Tipo: sequência

ResourceType

O tipo de AWS recurso salvo como ponto de recuperação; por exemplo, um volume do Amazon EBS ou um banco de dados do Amazon RDS.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna metadados associados a um ponto de recuperação, incluindo o ID, o status, a criptografia e o ciclo de vida.

Sintaxe da Solicitação

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

BackupVaultAccountId

O ID da conta do cofre de backup especificado.

Padrão: `^[0-9]{12}$`

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

recoveryPointArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupSizeInBytes

O tamanho de um backup, em bytes.

Tipo: longo

BackupVaultArn

Um ARN que identifica de forma exclusiva um cofre de backup. Por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

CalculatedLifecycle

Um objeto `CalculatedLifecycle` contendo timestamps `DeleteAt` e `MoveToColdStorageAt`.

Tipo: objeto CalculatedLifecycle

CompletionDate

A data e hora em que um trabalho para criar um ponto de recuperação foi concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

CompositeMemberIdentifier

O identificador de um recurso em um grupo composto, como um ponto de recuperação aninhado (filho) pertencente a uma pilha composta (principal). O ID é transferido do ID lógico dentro de uma pilha.

Tipo: sequência

CreatedBy

Contém informações de identificação sobre a criação de um ponto de recuperação, incluindo o `BackupPlanArn`, o `BackupPlanId`, a `BackupPlanVersion` e o `BackupRuleId` do plano de backup usado para criá-lo.

Tipo: objeto RecoveryPointCreator

CreationDate

A data e hora em que um ponto de recuperação foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

EncryptionKeyArn

A chave de criptografia no lado do servidor usada para proteger seus backups. Por exemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: sequência

IamRoleArn

Especifica o ARN do perfil do IAM usado para criar o ponto de recuperação de destino. Por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: sequência

IsEncrypted

Um valor booliano que é retornado como `TRUE` se o ponto de recuperação especificado estiver criptografado ou `FALSE` se o ponto de recuperação não estiver criptografado.

Tipo: booliano

IsParent

Isso retorna o valor booliano de que um ponto de recuperação é um trabalho pai (composto).

Tipo: booliano

LastRestoreTime

A data e hora em que um ponto de recuperação foi restaurado pela última vez, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastRestoreTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Lifecycle

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento refrigerado e quando ele expira. AWS Backup faz a transição e expira os backups automaticamente de acordo com o ciclo de vida definido por você.

Os backups transferidos para o armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias maior do que a configuração de “número de dias para transição para armazenamento frio”. A configuração de "número de dias para transferência ao armazenamento 'frio'" não poderá ser alterada depois que um backup for transferido para o armazenamento "frio".

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Tipo: objeto Lifecycle

ParentRecoveryPointArn

Isso é um ARN que identifica de forma exclusiva um ponto de recuperação pai (composto). Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

RecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

ResourceArn

Um ARN identifica de forma exclusiva um recurso salvo. O formato do ARN depende do tipo de recurso.

Tipo: sequência

ResourceName

O nome do recurso que pertence ao backup especificado.

Tipo: sequência

ResourceType

O tipo de AWS recurso a ser salvo como ponto de recuperação; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

SourceBackupVaultArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva o cofre de origem em que o backup do recurso foi feito originalmente. Por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`. Se a recuperação for restaurada na mesma AWS conta ou região, esse valor será`null`.

Tipo: sequência

Status

Um código de status que especifica o estado do ponto de recuperação.

`PARTIAL`o status indica que não AWS Backup foi possível criar o ponto de recuperação antes que a janela de backup fosse fechada. Para aumentar a janela do seu plano de backup usando

a API, consulte UpdateBackupPlan. Você também pode aumentar a janela do plano de backup usando o console, escolhendo e editando o plano de backup.

`EXPIRED`o status indica que o ponto de recuperação excedeu seu período de retenção, mas AWS Backup não tem permissão ou não consegue excluí-lo. Para excluir manualmente esses pontos de recuperação, consulte Etapa 3: Excluir os pontos de recuperação na seção Limpar recursos da Introdução.

O status `STOPPED` ocorre em um backup contínuo em que um usuário executou alguma ação que faz com que o backup contínuo seja desativado. Isso pode ser causado pela remoção de permissões, pela desativação do controle de versão, pela desativação do envio de EventBridge eventos ou pela desativação das EventBridge regras estabelecidas pelo. AWS Backup

Para resolver o status `STOPPED`, certifique-se de que todas as permissões solicitadas estejam em vigor e que o versionamento esteja habilitado no bucket do S3. Quando essas condições forem atendidas, a próxima instância de uma regra de backup em execução resultará na criação de um ponto de recuperação contínuo. Os pontos de recuperação com status PARADO não precisam ser excluídos.

Para o SAP HANA no Amazon EC2, o status `STOPPED` ocorre devido à ação do usuário, à configuração incorreta da aplicação ou à falha no backup. Para garantir que futuros backups contínuos tenham êxito, consulte o status do ponto de recuperação e verifique o SAP HANA para obter detalhes.

Tipo: sequências

Valores Válidos: `COMPLETED | PARTIAL | DELETING | EXPIRED`

StatusMessage

Uma mensagem de status explicando o status do ponto de recuperação.

Tipo: sequência

StorageClass

Especifica a classe de armazenamento do ponto de recuperação. Os valores válidos são `WARM` ou `COLD`.

Tipo: sequências

Valores Válidos: `WARM | COLD | DELETED`

VaultType

O tipo de cofre no qual o ponto de recuperação descrito é armazenado.

Tipo: sequências

Valores Válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna as configurações atuais da inclusão do serviço para a região. Se a aceitação do serviço estiver habilitada para um serviço, AWS Backup tentará proteger os recursos desse serviço nessa região, quando o recurso estiver incluído em um backup sob demanda ou em um plano de backup agendado. Caso contrário, o AWS Backup não tentará proteger os recursos desse serviço nessa região.

Sintaxe da Solicitação

```
GET /account-settings HTTP/1.1
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

ResourceTypeManagementPreference

Retorna se gerencia AWS Backup totalmente os backups de um tipo de recurso.

Para obter os benefícios do AWS Backup gerenciamento completo, consulte AWS Backup Gerenciamento completo.

Para obter uma lista dos tipos de recursos e se cada um oferece suporte ao AWS Backup gerenciamento completo, consulte a tabela Disponibilidade de recursos por recurso.

Se`"DynamoDB":false`, você pode habilitar o AWS Backup gerenciamento completo do backup do DynamoDB ativando os recursos avançados de backup AWS Backup do DynamoDB.

Tipo: mapa de string para booliano

Padrão da chave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ResourceTypeOptInPreference

Os serviços, juntamente com as preferências de aceitação na região.

Tipo: mapa de string para booliano

Padrão da chave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna os detalhes associados à criação de um relatório conforme especificado por seu `ReportJobId`.

Sintaxe da Solicitação

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

reportJobId

O identificador do trabalho de relatório. Uma string Unicode exclusiva, gerada aleatoriamente, codificada em UTF-8, com, no máximo, 1.024 bytes. Não é possível editar o ID do trabalho de relatório.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

ReportJob

As informações sobre um trabalho de relatório, incluindo seus horários de conclusão e criação, destino do relatório, ID exclusivo do trabalho de relatório, nome de recurso da Amazon (ARN), modelo de relatório, status e mensagem de status.

Tipo: objeto ReportJob

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma lista de todos os planos de relatório para um Conta da AWS Região da AWS e.

Sintaxe da Solicitação

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

reportPlanName

O nome exclusivo de um plano de relatório.

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Exigido: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

ReportPlan

Retorna detalhes sobre o plano de relatório especificado por seu nome. Esses detalhes incluem o Nome do recurso da Amazon (ARN) do plano de relatório, a descrição, as configurações, o canal de entrega, o status da implantação, o horário de criação, última tentativa dos tempos de execução e os tempos de execução com êxito.

Tipo: objeto ReportPlan

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna metadados associados a um trabalho de restauração especificado por um ID de trabalho.

Sintaxe da Solicitação

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

restoreJobId

Identifica de forma exclusiva o trabalho que restaura um ponto de recuperação.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AccountId

Retorna o ID da conta da que é proprietária do trabalho de restauração.

Tipo: string

Padrão: `^[0-9]{12}$`

BackupSizeInBytes

O tamanho, em bytes, do recurso restaurado.

Tipo: longo

CompletionDate

A data e a hora em que um trabalho para restaurar um ponto de recuperação foi concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

CreatedBy

Contém informações de identificação sobre a criação de um trabalho de restauração.

Tipo: objeto RestoreJobCreator

CreatedResourceArn

O Amazon Resource Name (ARN) do recurso que foi criado pela tarefa de restauração.

O formato do ARN depende do tipo de recurso que está tendo o backup feito.

Tipo: sequência

CreationDate

A data e hora em que a lista de domínios foi criada, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

DeletionStatus

O status dos dados gerados pelo teste de restauração.

Tipo: sequências

Valores Válidos: `DELETING | FAILED | SUCCESSFUL`

DeletionStatusMessage

Isso descreve o status de exclusão do trabalho de restauração.

Tipo: sequência

ExpectedCompletionTimeMinutes

A quantidade de tempo, em minutos, que se espera que um trabalho de restauração de um ponto de recuperação leve.

Tipo: longo

IamRoleArn

Especifica o ARN do perfil do IAM usado para criar o ponto de recuperação de destino. Por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: sequência

PercentDone

Contém uma porcentagem estimada de conclusão de um trabalho no momento em que o status do trabalho foi consultado.

Tipo: sequência

RecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

RecoveryPointCreationDate

A data de criação do ponto de recuperação criado pela tarefa de restauração especificada.

Tipo: carimbo de data/hora

ResourceType

Retorna metadados associados a um trabalho de restauração listado por tipo de recurso.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreJobId

Identifica de forma exclusiva o trabalho que restaura um ponto de recuperação.

Tipo: sequência

Status

Código de status que especifica o estado do trabalho que é iniciado AWS Backup para restaurar um ponto de recuperação.

Tipo: sequências

Valores Válidos: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

StatusMessage

Uma mensagem mostrando o status de um trabalho para restaurar um ponto de recuperação.

Tipo: sequência

ValidationStatus

O status da validação executada na tarefa de restauração indicada.

Tipo: sequências

Valores Válidos: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

ValidationStatusMessage

A mensagem de status.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

DependencyFailureException

Um AWS serviço ou recurso dependente retornou um erro ao AWS Backup serviço e a ação não pode ser concluída.

Código de Status HTTP: 500

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui o ponto de recuperação de backup contínuo especificado AWS Backup e libera o controle desse backup contínuo para o serviço de origem, como o Amazon RDS. O serviço de origem continuará criando e retendo backups contínuos usando o ciclo de vida que você especificou em seu plano de backup original.

Não é compatível com pontos de recuperação de backup de snapshots.

Sintaxe da Solicitação

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome exclusivo de um AWS Backup cofre.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

recoveryPointArn

Um nome de recurso da Amazon (ARN) que identifica de forma exclusiva um ponto de recuperação. AWS Backup

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

InvalidResourceStateException

AWS Backup já está executando uma ação nesse ponto de recuperação. Ele não pode realizar a ação solicitada até que a primeira ação seja concluída. Tente novamente mais tarde.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa ação para um ponto de recuperação filho específico (aninhado) remove o relacionamento entre o ponto de recuperação especificado e seu ponto de recuperação pai (composto).

Sintaxe da Solicitação

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico em que o ponto de recuperação filho (aninhado) é armazenado. Os cofres de backup são identificados por nomes exclusivos da conta usada para criá-los e da AWS região em que foram criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

recoveryPointArn

O Amazon Resource Name (ARN) que identifica de forma exclusiva o ponto de recuperação secundário (aninhado); por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 204
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 204 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna o plano de backup especificado pelo ID do plano como um modelo de backup.

Sintaxe da Solicitação

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupPlanId

Identifica exclusivamente um plano de backup.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupPlanTemplateJson

O corpo de um modelo de plano de backup no formato JSON.

> **Note**
>
> Isso é um documento JSON assinado que não pode ser modificado antes de ser passado para `GetBackupPlanFromJSON`.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface

- 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

Serviço: AWS Backup

Retorna detalhes do `BackupPlan` do `BackupPlanId` especificado. Os detalhes são o corpo de um plano de backup no formato JSON, além dos metadados do plano.

Sintaxe da Solicitação

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupPlanId

Identifica exclusivamente um plano de backup.

Obrigatório: Sim

VersionId

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. IDs de versão não podem ser editados.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AdvancedBackupSettings

Contém uma lista de `BackupOptions` para cada tipo de recurso. A lista será preenchida somente se a opção avançada estiver definida para o plano de backup.

Tipo: matriz de objetos AdvancedBackupSetting

BackupPlan

Especifica o corpo de um plano de backup. Inclui um `BackupPlanName` e um ou mais conjuntos de `Rules`.

Tipo: objeto BackupPlan

BackupPlanArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um plano de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: sequência

BackupPlanId

Identifica exclusivamente um plano de backup.

Tipo: sequência

CreationDate

A data e hora em que o plano de backup foi criado, em formato de hora Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

CreatorRequestId

Uma string que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes.

Tipo: sequência

DeletionDate

A data e hora em que um plano de backup foi excluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `DeletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

LastExecutionDate

A última vez que esse plano de backup foi executado. A data e a hora devem estar em formato Unix e UTC (Tempo Universal Coordenado). O valor de `LastExecutionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

VersionId

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. IDs de versão não podem ser editados.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna um documento JSON válido especificando um plano de backup ou um erro.

Sintaxe da Solicitação

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

BackupPlanTemplateJson

Um documento de plano de backup fornecido pelo cliente no formato JSON.

Tipo: string

Obrigatório: Sim

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupPlan

Especifica o corpo de um plano de backup. Inclui um `BackupPlanName` e um ou mais conjuntos de `Rules`.

Tipo: objeto BackupPlan

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna o modelo especificado por seu `templateId` como um plano de backup.

Sintaxe da Solicitação

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

templateId

Identifica de forma exclusiva um modelo de plano de backup armazenado.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupPlanDocument

Retorna o corpo de um plano de backup com base no modelo de destino, incluindo o nome, as regras e o cofre de backup do plano.

Tipo: objeto BackupPlan

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna metadados de seleção e um documento no formato JSON que especifica uma lista de recursos associados a um plano de backup.

Sintaxe da Solicitação

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupPlanId

Identifica exclusivamente um plano de backup.

Obrigatório: Sim

selectionId

Identifica de forma exclusiva uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupPlanId

Identifica exclusivamente um plano de backup.

Tipo: sequência

BackupSelection

Especifica o corpo de uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Tipo: objeto BackupSelection

CreationDate

A data e hora em que uma seleção de backup foi criada, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

CreatorRequestId

Uma string que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes.

Tipo: sequência

SelectionId

Identifica de forma exclusiva uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna o documento de política de acesso associado ao cofre de backup nomeado.

Sintaxe da Solicitação

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupVaultArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Policy

O documento da política de acesso ao cofre de backup no formato JSON.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Exclui as notificações de eventos para o cofre de backup especificado.

Sintaxe da Solicitação

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupVaultArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

BackupVaultEvents

Uma matriz de eventos que indicam o status de trabalhos para recursos de backup para o cofre de backup.

Tipo: matriz de strings

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

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

SNSTopicArn

Um ARN que identifica exclusivamente um tópico do Amazon Simple Notification Service (Amazon SNS); por exemplo, `arn:aws:sns:us-west-2:111122223333:MyTopic`.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa ação retorna detalhes de uma retenção legal especificada. Os detalhes são o corpo de uma retenção legal no formato JSON, além dos metadados.

Sintaxe da Solicitação

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

legalHoldId

O ID da retenção legal.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CancelDescription

O motivo da remoção da retenção legal.

Tipo: sequência

CancellationDate

A hora em que a retenção legal foi cancelada.

Tipo: carimbo de data/hora

CreationDate

A hora em que a retenção legal foi criada.

Tipo: carimbo de data/hora

Description

A descrição da retenção legal.

Tipo: sequência

LegalHoldArn

O ARN da estrutura para a retenção legal especificada. O formato do ARN depende do tipo de recurso.

Tipo: sequência

LegalHoldId

O ID da retenção legal.

Tipo: sequência

RecoveryPointSelection

Os critérios para atribuir um conjunto de recursos, como tipos de recursos ou cofres de backup.

Tipo: objeto RecoveryPointSelection

RetainRecordUntil

A data e a hora até as quais o registro legal de retenção é retido.

Tipo: carimbo de data/hora

Status

O status da retenção legal.

Tipo: sequências

Valores Válidos: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

O título da retenção legal.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna um conjunto de pares de chave/valor de metadados que foram usados para criar o backup.

Sintaxe da Solicitação

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

BackupVaultAccountId

O ID da conta do cofre de backup especificado.

Padrão: `^[0-9]{12}$`

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

recoveryPointArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupVaultArn

Um ARN que identifica de forma exclusiva um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

RecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

ResourceType

O tipo de recurso do ponto de recuperação.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreMetadata

O conjunto de pares de chave/valor de metadados que descrevem a configuração original do recurso que teve o backup feito. Esses valores variam dependendo do serviço que está sendo restaurado.

Tipo: mapa de string para string

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface

- 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

Serviço: AWS Backup

Essa solicitação retorna os metadados do trabalho de restauração especificado.

Sintaxe da Solicitação

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

restoreJobId

Esse é um identificador exclusivo de um trabalho de restauração interno AWS Backup.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Metadata

Isso contém os metadados do trabalho de backup especificado.

Tipo: mapa de string para string

RestoreJobId

Esse é um identificador exclusivo de um trabalho de restauração interno AWS Backup.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa solicitação retorna o conjunto mínimo de metadados necessário para iniciar um trabalho de restauração com configurações padrão seguras. `BackupVaultName` e `RecoveryPointArn` são parâmetros obrigatórios. `BackupVaultAccountId` é um parâmetro opcional.

Sintaxe da Solicitação

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

BackupVaultAccountId

O ID da conta do cofre de backup especificado.

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes exclusivos da conta usada para criá-los e da AWS região em que foram criados. Eles consistem em letras, números e hifens.

Obrigatório: Sim

RecoveryPointArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

InferredMetadata

Isso é um mapa de strings dos metadados inferidos da solicitação.

Tipo: mapa de string para string

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna detalhes do `RestoreTestingPlan` do `RestoreTestingPlanName` especificado. Os detalhes são o corpo de um plano de testes de restauração no formato JSON, além dos metadados do plano.

Sintaxe da Solicitação

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

RestoreTestingPlanName

Nome exclusivo obrigatório do plano de testes de restauração.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

RestoreTestingPlan

Especifica o corpo de um plano de testes de restauração. Inclui `RestoreTestingPlanName`.

Tipo: objeto RestoreTestingPlanForGet

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface

- 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

Serviço: AWS Backup

Retorna RestoreTestingSelection, que exibe recursos e elementos do plano de teste de restauração.

Sintaxe da Solicitação

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

RestoreTestingPlanName

Nome exclusivo obrigatório do plano de testes de restauração.

Obrigatório: Sim

RestoreTestingSelectionName

Nome exclusivo obrigatório da seleção de testes de restauração.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

RestoreTestingSelection

Nome exclusivo da seleção de testes de restauração.

Tipo: objeto RestoreTestingSelectionForGet

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna os tipos de AWS recursos suportados pelo AWS Backup.

Sintaxe da Solicitação

```
GET /supported-resource-types HTTP/1.1
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

ResourceTypes

Contém uma string com os tipos AWS de recursos compatíveis:

- `Aurora` para Amazon Aurora
- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (compatível com MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store

- `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 bancos de dados SAP HANA em instâncias do Amazon Elastic Compute Cloud
- `S3`para o Amazon Simple Storage Service (Amazon S3)
- `Storage Gateway`para AWS Storage Gateway
- `Timestream` para Amazon Timestream
- `VirtualMachine`para máquinas virtuais VMware

Tipo: matriz de strings

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma lista dos trabalhos de backup existentes para uma conta autenticada nos últimos 30 dias. Para um período mais longo, considere usar essas ferramentas de monitoramento.

Sintaxe da Solicitação

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

ByAccountId

O ID da conta a partir da qual listar os trabalhos. Retorna somente os trabalhos de backup associados ao ID da conta especificado.

Se usado em uma conta AWS Organizations de gerenciamento, o passe * retorna todos os trabalhos em toda a organização.

Padrão: `^[0-9]{12}$`

ByBackupVaultName

Retorna somente os trabalhos de backup que serão armazenados no cofre de backup especificado. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

ByCompleteAfter

Retorna somente os trabalhos de backup concluídos após uma data expressa em formato Unix e Tempo Universal Coordenado (UTC).

ByCompleteBefore

Retorna somente os trabalhos de backup concluídos antes de uma data expressa em formato Unix e Tempo Universal Coordenado (UTC).

ByCreatedAfter

Retorna somente os trabalhos de backup que foram criados após a data especificada.

ByCreatedBefore

Retorna somente os trabalhos de backup que foram criados antes da data especificada.

ByMessageCategory

Esse é um parâmetro opcional que pode ser usado para filtrar trabalhos com um valor MessageCategory que corresponda ao valor inserido.

Exemplos de strings podem incluir `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `InvalidParameters`.

Consulte Monitoring.

O curinga (*) retorna a contagem de todas as categorias de mensagens.

`AGGREGATE_ALL` agrega as contagens de trabalhos de todas as categorias de mensagens e retorna a soma.

ByParentJobId

Isso é um filtro para listar os trabalhos filho (aninhados) com base no ID do trabalho pai.

ByResourceArn

Retorna somente os trabalhos de backup que correspondam ao Nome do recurso da Amazon (ARN) do recurso especificado.

ByResourceType

Retorna somente os trabalhos de backup para os recursos especificados:

- `Aurora` para Amazon Aurora
- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (compatível com MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store
- `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 bancos de dados SAP HANA
- `Storage Gateway`para AWS Storage Gateway
- `S3` para Amazon S3
- `Timestream` para Amazon Timestream
- `VirtualMachine` para máquinas virtuais

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Retorna somente os trabalhos de backup que estejam no estado especificado.

`Completed with issues` é um status encontrado somente no console do AWS Backup . Para a API, esse status se refere a trabalhos com um estado de `COMPLETED` e a uma `MessageCategory` com um valor diferente de `SUCCESS`, o que significa que o status é Concluído, mas vem com uma mensagem de status.

Para obter a contagem de trabalhos `Completed with issues`, execute duas solicitações GET e subtraia o número menor:

GET /backup-jobs/?state=COMPLETED

GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED

Valores Válidos: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupJobs

Uma matriz de estruturas contendo metadados sobre os trabalhos de backup retornados no formato JSON.

Tipo: matriz de objetos BackupJob

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa é uma solicitação para um resumo dos trabalhos de backup criados ou em execução nos últimos 30 dias. Você pode incluir os parâmetros AccountId, State,,, ResourceType, MessageCategory AggregationPeriod MaxResults, NextToken ou para filtrar os resultados.

Essa solicitação retorna um resumo que contém região, conta, estado ResourceType, MessageCategory, StartTime, EndTime, e contagem de trabalhos incluídos.

Sintaxe da Solicitação

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

AccountId

Retorna a contagem de trabalhos para a conta especificada.

Se a solicitação for enviada de uma conta de membro ou de uma conta que não faz parte de AWS Organizations, os trabalhos na conta do solicitante serão devolvidos.

As contas raiz, de administrador e de administrador delegado podem usar o valor ANY para retornar as contagens de trabalhos de todas as contas da organização.

AGGREGATE_ALL agrega as contagens de trabalhos de todas as contas da organização autenticada e retorna a soma.

Padrão: `^[0-9]{12}$`

AggregationPeriod

O período para os resultados retornados.

- ONE_DAY- A contagem diária de trabalhos dos 14 dias anteriores.
- SEVEN_DAYS- A contagem agregada de trabalhos dos 7 dias anteriores.

- FOURTEEN_DAYS- A contagem agregada de empregos dos 14 dias anteriores.

Valores Válidos: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

O número máximo de itens a serem retornados.

O valor é um inteiro. O intervalo de valores aceitos é de 1 a 500.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

MessageCategory

Esse parâmetro retorna a contagem de trabalhos para a categoria de mensagem especificada.

Exemplos de strings aceitas incluem `AccessDenied`, `Success` e `InvalidParameters`. Consulte Monitoramento para obter uma lista de MessageCategory sequências de caracteres aceitas.

O valor ANY retorna a contagem de todas as categorias de mensagens.

`AGGREGATE_ALL` agrega as contagens de trabalhos de todas as categorias de mensagens e retorna a soma.

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `MaxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

ResourceType

Retorna a contagem de trabalhos para o tipo de recurso especificado. Use a solicitação `GetSupportedResourceTypes` a fim de obter as strings para os tipos de recurso compatíveis.

O valor ANY retorna a contagem de todos os tipos de recurso.

`AGGREGATE_ALL` agrega as contagens de trabalhos para todos os tipos de recurso e retorna a soma.

O tipo de AWS recurso a ser copiado; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Esse parâmetro retorna a contagem dos trabalhos que estão no estado especificado.

O valor ANY retorna a contagem de todos os estados.

AGGREGATE_ALL agrega as contagens de trabalhos para todos os estados e retorna a soma.

Completed with issues é um status encontrado somente no console do AWS Backup . Para a API, esse status se refere a trabalhos com um estado de COMPLETED e a uma MessageCategory com um valor diferente de SUCCESS, o que significa que o status é Concluído, mas vem com uma mensagem de status. Para obter a contagem de trabalhos Completed with issues, execute duas solicitações GET e subtraia o número menor:

OBTENHA /audit/backup-job-summaries? AggregationPeriod=Quatorze_dias&state=Concluído

OBTENHA /audit/backup-job-summaries? AggregationPeriod=FOURTEEN_DAYS& MessageCategory =SUCESSO&STATE=Concluído

Valores Válidos: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AggregationPeriod

O período para os resultados retornados.

- ONE_DAY- A contagem diária de trabalhos dos 14 dias anteriores.
- SEVEN_DAYS- A contagem agregada de trabalhos dos 7 dias anteriores.
- FOURTEEN_DAYS- A contagem agregada de empregos dos 14 dias anteriores.

Tipo: sequência

BackupJobSummaries

As informações resumidas.

Tipo: matriz de objetos BackupJobSummary

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `MaxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Lista os planos de backup ativos da conta.

Sintaxe da Solicitação

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

IncludeDeleted

Um valor booliano com um valor padrão de `FALSE` que retorna os planos de backup excluídos quando definido como `TRUE`.

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupPlansList

Informações sobre os planos de backup.

Tipo: matriz de objetos BackupPlansListMember

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Lista os modelos do plano de backup.

Sintaxe da Solicitação

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

MaxResults

O número máximo de itens a serem devolvidos.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
   "NextToken": "string"
```

```
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupPlanTemplatesList

Uma matriz de itens da lista de modelos contendo metadados sobre seus modelos salvos.

Tipo: matriz de objetos BackupPlanTemplatesListMember

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna metadados da versão de seus planos de backup, incluindo Nomes de recurso da Amazon (ARNs), IDs de planos de backup, datas de criação e exclusão, nomes de planos e IDs de versão.

Sintaxe da Solicitação

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupPlanId

Identifica exclusivamente um plano de backup.

Obrigatório: Sim

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupPlanVersionsList

Uma matriz de itens da lista de versões contendo metadados sobre seus planos de backup.

Tipo: matriz de objetos BackupPlansListMember

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma matriz contendo metadados dos recursos associados ao plano de backup de destino.

Sintaxe da Solicitação

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupPlanId

Identifica exclusivamente um plano de backup.

Obrigatório: Sim

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupSelectionsList

Uma matriz de itens da lista de seleção de backup contendo metadados sobre cada recurso na lista.

Tipo: matriz de objetos BackupSelectionsListMember

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma lista de contêineres de armazenamento de pontos de recuperação junto com informações sobre eles.

Sintaxe da Solicitação

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

ByShared

Esse parâmetro classificará a lista de cofres por cofres compartilhados.

ByVaultType

Esse parâmetro classificará a lista de cofres por tipo de cofre.

Valores Válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupVaultList

Uma matriz de membros da lista de cofres de backup contendo metadados do cofre, incluindo o Nome do recurso da Amazon (ARN), o nome de exibição, a data de criação, o número de pontos de recuperação salvos e informações de criptografia se os recursos salvos no cofre de backup estiverem criptografados.

Tipo: matriz de objetos BackupVaultListMember

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna metadados sobre seus trabalhos de cópia.

Sintaxe da Solicitação

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

ByAccountId

O ID da conta a partir da qual listar os trabalhos. Retorna somente os trabalhos de cópia associados ao ID da conta especificada.

Padrão: `^[0-9]{12}$`

ByCompleteAfter

Retorna somente os trabalhos de cópia concluídos após uma data expressa em formato Unix e Tempo Universal Coordenado (UTC).

ByCompleteBefore

Retorna somente os trabalhos de cópia concluídos após uma data expressa em formato Unix e Tempo Universal Coordenado (UTC).

ByCreatedAfter

Retorna somente os trabalhos de cópia que foram criados após a data especificada.

ByCreatedBefore

Retorna somente os trabalhos de cópia que foram criados antes da data especificada.

ByDestinationVaultArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

ByMessageCategory

Esse é um parâmetro opcional que pode ser usado para filtrar trabalhos com um valor MessageCategory que corresponda ao valor inserido.

Exemplos de strings podem incluir `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `INVALIDPARAMETERS`.

Consulte Monitoring para conferir uma lista de strings aceitas.

O valor ANY retorna a contagem de todas as categorias de mensagens.

`AGGREGATE_ALL` agrega as contagens de trabalhos de todas as categorias de mensagens e retorna a soma.

ByParentJobId

Isso é um filtro para listar os trabalhos filho (aninhados) com base no ID do trabalho pai.

ByResourceArn

Retorna somente os trabalhos de cópia que correspondam ao Nome do recurso da Amazon (ARN) especificado.

ByResourceType

Retorna somente os trabalhos de backup para os recursos especificados:

- `Aurora` para Amazon Aurora
- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (compatível com MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store
- `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 bancos de dados SAP HANA
- `Storage Gateway`para AWS Storage Gateway

- `S3` para Amazon S3
- `Timestream` para Amazon Timestream
- `VirtualMachine` para máquinas virtuais

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Retorna somente os trabalhos de cópia que estão no estado especificado.

Valores Válidos: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para devolver o MaxResults número de NextToken itens, você poderá devolver mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CopyJobs

Uma matriz de estruturas contendo metadados sobre seus trabalhos de cópia retornados no formato JSON.

Tipo: matriz de objetos CopyJob

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para devolver o MaxResults número de NextToken itens, você poderá devolver mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa solicitação obtém uma lista dos trabalhos de cópia criados ou em execução nos últimos 30 dias. Você pode incluir os parâmetros AccountId, State,,, ResourceType, MessageCategory AggregationPeriod MaxResults, NextToken ou para filtrar os resultados.

Essa solicitação retorna um resumo que contém Região, Conta, Estado, RestourceType, MessageCategory, StartTime EndTime, e Contagem dos trabalhos incluídos.

Sintaxe da Solicitação

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

AccountId

Retorna a contagem de trabalhos para a conta especificada.

Se a solicitação for enviada de uma conta de membro ou de uma conta que não faz parte de AWS Organizations, os trabalhos na conta do solicitante serão devolvidos.

As contas raiz, de administrador e de administrador delegado podem usar o valor ANY para retornar as contagens de trabalhos de todas as contas da organização.

`AGGREGATE_ALL` agrega as contagens de trabalhos de todas as contas da organização autenticada e retorna a soma.

Padrão: `^[0-9]{12}$`

AggregationPeriod

O período para os resultados retornados.

- `ONE_DAY`- A contagem diária de trabalhos dos 14 dias anteriores.
- `SEVEN_DAYS`- A contagem agregada de trabalhos dos 7 dias anteriores.

- FOURTEEN_DAYS- A contagem agregada de empregos dos 14 dias anteriores.

Valores Válidos: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

Esse parâmetro define o número máximo de itens a serem retornados.

O valor é um inteiro. O intervalo de valores aceitos é de 1 a 500.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

MessageCategory

Esse parâmetro retorna a contagem de trabalhos para a categoria de mensagem especificada.

Exemplos de strings aceitas incluem AccessDenied, Success e InvalidParameters. Consulte Monitoramento para obter uma lista de MessageCategory sequências de caracteres aceitas.

O valor ANY retorna a contagem de todas as categorias de mensagens.

AGGREGATE_ALL agrega as contagens de trabalhos de todas as categorias de mensagens e retorna a soma.

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número MaxResults de recursos, o NextToken permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

ResourceType

Retorna a contagem de trabalhos para o tipo de recurso especificado. Use a solicitação GetSupportedResourceTypes a fim de obter as strings para os tipos de recurso compatíveis.

O valor ANY retorna a contagem de todos os tipos de recurso.

AGGREGATE_ALL agrega as contagens de trabalhos para todos os tipos de recurso e retorna a soma.

O tipo de AWS recurso a ser copiado; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Esse parâmetro retorna a contagem dos trabalhos que estão no estado especificado.

O valor ANY retorna a contagem de todos os estados.

AGGREGATE_ALL agrega as contagens de trabalhos para todos os estados e retorna a soma.

Valores Válidos: `CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY`

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AggregationPeriod

O período para os resultados retornados.

- `ONE_DAY`- A contagem diária de trabalhos dos 14 dias anteriores.
- `SEVEN_DAYS`- A contagem agregada de trabalhos dos 7 dias anteriores.
- `FOURTEEN_DAYS`- A contagem agregada de empregos dos 14 dias anteriores.

Tipo: sequência

CopyJobSummaries

Essa devolução mostra um resumo que contém região, conta, estado ResourceType, MessageCategory, StartTime, EndTime, e contagem de trabalhos incluídos.

Tipo: matriz de objetos CopyJobSummary

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `MaxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma lista de todas as estruturas de um Conta da AWS e. Região da AWS

Sintaxe da Solicitação

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

MaxResults

O número de resultados desejados de 1 a 1.000. Opcional. Se não for especificado, a consulta retornará 1 MB de dados.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

NextToken

Um identificador que foi retornado da chamada anterior para essa operação, que pode ser usado para retornar o próximo conjunto de itens na lista.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Frameworks

As estruturas com detalhes de cada estrutura, incluindo o nome da estrutura, o Amazon Resource Name (ARN), a descrição, o número de controles, o horário de criação e o status da implantação.

Tipo: matriz de objetos Framework

NextToken

Um identificador que foi retornado da chamada anterior para essa operação, que pode ser usado para retornar o próximo conjunto de itens na lista.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa ação retorna metadados sobre retenções legais ativas e anteriores.

Sintaxe da Solicitação

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

MaxResults

O número máximo de itens da lista de recursos a serem retornados.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `MaxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

LegalHolds

Isso é uma matriz de retenções legais retornadas, tanto ativas quanto anteriores.

Tipo: matriz de objetos LegalHold

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `MaxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma matriz de recursos com backup bem-sucedido AWS Backup, incluindo o tempo em que o recurso foi salvo, um Amazon Resource Name (ARN) do recurso e um tipo de recurso.

Sintaxe da Solicitação

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Results

Um conjunto de recursos foi copiado com sucesso AWS Backup , incluindo o tempo em que o recurso foi salvo, um nome de recurso da Amazon (ARN) do recurso e um tipo de recurso.

Tipo: matriz de objetos ProtectedResource

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa solicitação lista os recursos protegidos correspondentes a cada cofre de backup.

Sintaxe da Solicitação

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

BackupVaultAccountId

A lista de recursos protegidos pelo cofre de backup dentro do (s) cofre (s) especificado (s) por ID da conta.

Padrão: `^[0-9]{12}$`

backupVaultName

A lista de recursos protegidos pelo cofre de backup dentro do (s) cofre (s) especificado (s) por nome.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Results

Esses são os resultados retornados para a solicitação ListProtectedResourcesByBackupVault.

Tipo: matriz de objetos ProtectedResource

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna informações detalhadas sobre os pontos de recuperação armazenados em um cofre de backup.

Sintaxe da Solicitação

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

BackupVaultAccountId

Esse parâmetro classificará a lista de pontos de recuperação por ID de conta.

Padrão: `^[0-9]{12}$`

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

> **Note**
>
> O nome do cofre de backup pode não estar disponível quando um serviço compatível cria o backup.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

ByBackupPlanId

Retorna somente os pontos de recuperação que correspondam ao ID do plano de backup especificado.

ByCreatedAfter

Retorna somente os pontos de recuperação que foram criados após o timestamp especificado.

ByCreatedBefore

Retorna somente os pontos de recuperação que foram criados antes do timestamp especificado.

ByParentRecoveryPointArn

Isso retorna somente os pontos de recuperação que correspondem ao Nome do recurso da Amazon (ARN) do ponto de recuperação pai (composto) especificado.

ByResourceArn

Retorna somente os pontos de recuperação que correspondem ao Nome do recurso da Amazon (ARN) do recurso especificado.

ByResourceType

Retorna somente os pontos de recuperação que correspondem aos tipos de recurso especificados:

- `Aurora` para Amazon Aurora
- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (compatível com MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store
- `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 bancos de dados SAP HANA
- `Storage Gateway`para AWS Storage Gateway
- `S3` para Amazon S3
- `Timestream` para Amazon Timestream

- `VirtualMachine` para máquinas virtuais

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

RecoveryPoints

Uma matriz de objetos que contém informações detalhadas sobre os pontos de recuperação salvos em um cofre de backup.

Tipo: matriz de objetos RecoveryPointByBackupVault

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa ação retorna os Nomes do recurso da Amazon (ARNs) do ponto de recuperação da retenção legal especificada.

Sintaxe da Solicitação

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

legalHoldId

O ID da retenção legal.

Obrigatório: Sim

MaxResults

O número máximo de itens da lista de recursos a serem retornados.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `MaxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos recursos retornados.

Tipo: sequência

RecoveryPoints

Os pontos de recuperação.

Tipo: matriz de objetos RecoveryPointMember

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

As informações sobre os pontos de recuperação do tipo especificado por um recurso Amazon Resource Name (ARN).

> **Note**
>
> Para o Amazon EFS e o Amazon EC2, essa ação lista somente os pontos de recuperação criados pelo AWS Backup.

Sintaxe da Solicitação

```
GET /resources/resourceArn/recovery-points/?
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

ManagedByAWSBackupOnly

Esse atributo filtra os pontos de recuperação com base na propriedade.

Se estiver definido como`TRUE`, a resposta conterá pontos de recuperação associados aos recursos selecionados que são gerenciados pelo AWS Backup.

Se estiver definido como`FALSE`, a resposta conterá todos os pontos de recuperação associados ao recurso selecionado.

Tipo: booliano

MaxResults

O número máximo de itens a serem retornados.

> **Note**
>
> O Amazon RDS exige um valor de pelo menos 20.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

resourceArn

Um ARN que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

RecoveryPoints

Uma matriz de objetos que contém informações detalhadas sobre os pontos de recuperação do tipo de recurso especificado.

> **Note**
>
> Somente os pontos de recuperação do Amazon EFS e do Amazon EC2 retornam. BackupVaultName

Tipo: matriz de objetos RecoveryPointByResource

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna detalhes sobre seus trabalhos de relatório.

Sintaxe da Solicitação

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

ByCreationAfter

Retorna somente trabalhos de relatório que foram criados após a data e hora especificadas em formato Unix e Tempo Universal Coordenado (UTC). Por exemplo, o valor 1516925490 representa sexta-feira, 26 de janeiro de 2018, 0:11:30.

ByCreationBefore

A data e hora em que um trabalho de restauração foi criado, em formato Unix e Tempo Universal Coordenado (UTC). Por exemplo, o valor 1516925490 representa sexta-feira, 26 de janeiro de 2018, 0:11:30.

ByReportPlanName

Retorna somente trabalhos de relatório com o nome do plano de relatório especificado.

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

Retorna somente trabalhos de relatório que estejam no status especificado. Os status são:

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

O número de resultados desejados de 1 a 1.000. Opcional. Se não for especificado, a consulta retornará 1 MB de dados.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

NextToken

Um identificador que foi retornado da chamada anterior para essa operação, que pode ser usado para retornar o próximo conjunto de itens na lista.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

Um identificador que foi retornado da chamada anterior para essa operação, que pode ser usado para retornar o próximo conjunto de itens na lista.

Tipo: sequência

ReportJobs

Os detalhes sobre seus trabalhos de relatório em formato JSON.

Tipo: matriz de objetos ReportJob

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma lista de seus planos de relatório. Para obter informações detalhadas sobre um único plano de relatório, use `DescribeReportPlan`.

Sintaxe da Solicitação

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

MaxResults

O número de resultados desejados de 1 a 1.000. Opcional. Se não for especificado, a consulta retornará 1 MB de dados.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

NextToken

Um identificador que foi retornado da chamada anterior para essa operação, que pode ser usado para retornar o próximo conjunto de itens na lista.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

Um identificador que foi retornado da chamada anterior para essa operação, que pode ser usado para retornar o próximo conjunto de itens na lista.

Tipo: sequência

ReportPlans

O relatório planeja com informações detalhadas para cada plano. Essas informações incluem o Nome do recurso da Amazon (ARN), o nome do plano de relatório, a descrição, as configurações, o canal de entrega, o status da implantação, a hora de criação e as últimas vezes em que o plano de relatório tentou e foi executado com êxito.

Tipo: matriz de objetos ReportPlan

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma lista de trabalhos AWS Backup iniciados para restaurar um recurso salvo, incluindo detalhes sobre o processo de recuperação.

Sintaxe da Solicitação

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

ByAccountId

O ID da conta a partir da qual listar os trabalhos. Retorna somente trabalhos de restauração associados ao ID da conta especificada.

Padrão: `^[0-9]{12}$`

ByCompleteAfter

Retorna somente os trabalhos de cópia concluídos após uma data expressa em formato Unix e Tempo Universal Coordenado (UTC).

ByCompleteBefore

Retorna somente os trabalhos de cópia concluídos após uma data expressa em formato Unix e Tempo Universal Coordenado (UTC).

ByCreatedAfter

Retorna somente trabalhos de restauração que foram criados após a data especificada.

ByCreatedBefore

Retorna somente trabalhos de restauração que foram criados antes da data especificada.

ByResourceType

Inclua esse parâmetro para retornar somente trabalhos de restauração para os recursos especificados:

- `Aurora` para Amazon Aurora

- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (compatível com MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store
- `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 bancos de dados SAP HANA
- `Storage Gateway`para AWS Storage Gateway
- `S3` para Amazon S3
- `Timestream` para Amazon Timestream
- `VirtualMachine` para máquinas virtuais

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByRestoreTestingPlanArn

Isso retorna somente os trabalhos de testes de restauração que correspondem ao nome do recurso da Amazon (ARN) especificado.

ByStatus

Retorna somente trabalhos de restauração associados ao status do trabalho especificado.

Valores Válidos: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

RestoreJobs

Uma matriz de objetos que contém informações detalhadas sobre trabalhos para restaurar recursos salvos.

Tipo: matriz de objetos RestoreJobsListMember

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Isso retorna os trabalhos de restauração que contêm o recurso protegido especificado.

Você deve incluir `ResourceArn`. Você também pode incluir `NextToken`, `ByStatus`, `MaxResults`, `ByRecoveryPointCreationDateAfter` e `ByRecoveryPointCreationDateBefore`.

Sintaxe da Solicitação

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

ByRecoveryPointCreationDateAfter

Retorna somente os trabalhos de restauração de pontos de recuperação que foram criados após a data especificada.

ByRecoveryPointCreationDateBefore

Retorna somente os trabalhos de restauração de pontos de recuperação que foram criados antes da data especificada.

ByStatus

Retorna somente trabalhos de restauração associados ao status do trabalho especificado.

Valores Válidos: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar a quantidade `MaxResults` de itens, `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

resourceArn

Retorna somente os trabalhos de restauração que correspondem ao nome do recurso da Amazon (ARN) especificado.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar a quantidade `MaxResults` de itens, `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

RestoreJobs

Uma matriz de objetos que contêm informações detalhadas sobre trabalhos para restaurar recursos salvos.

Tipo: matriz de objetos RestoreJobsListMember

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa solicitação obtém um resumo dos trabalhos de restauração criados ou em execução nos últimos 30 dias. Você pode incluir os parâmetros AccountId, State,,, ResourceType AggregationPeriod MaxResults, NextToken ou para filtrar os resultados.

Essa solicitação retorna um resumo que contém região, conta, estado RestourceType, MessageCategory, StartTime, EndTime, e contagem de trabalhos incluídos.

Sintaxe da Solicitação

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

AccountId

Retorna a contagem de trabalhos para a conta especificada.

Se a solicitação for enviada de uma conta de membro ou de uma conta que não faz parte de AWS Organizations, os trabalhos na conta do solicitante serão devolvidos.

As contas raiz, de administrador e de administrador delegado podem usar o valor ANY para retornar as contagens de trabalhos de todas as contas da organização.

AGGREGATE_ALL agrega as contagens de trabalhos de todas as contas da organização autenticada e retorna a soma.

Padrão: ^[0-9]{12}$

AggregationPeriod

O período para os resultados retornados.

- ONE_DAY- A contagem diária de trabalhos dos 14 dias anteriores.
- SEVEN_DAYS- A contagem agregada de trabalhos dos 7 dias anteriores.
- FOURTEEN_DAYS- A contagem agregada de empregos dos 14 dias anteriores.

Valores Válidos: `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Esse parâmetro define o número máximo de itens a serem retornados.

O valor é um inteiro. O intervalo de valores aceitos é de 1 a 500.

Faixa válida: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `MaxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

ResourceType

Retorna a contagem de trabalhos para o tipo de recurso especificado. Use a solicitação `GetSupportedResourceTypes` a fim de obter as strings para os tipos de recurso compatíveis.

O valor ANY retorna a contagem de todos os tipos de recurso.

`AGGREGATE_ALL` agrega as contagens de trabalhos para todos os tipos de recurso e retorna a soma.

O tipo de AWS recurso a ser copiado; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Esse parâmetro retorna a contagem dos trabalhos que estão no estado especificado.

O valor ANY retorna a contagem de todos os estados.

`AGGREGATE_ALL` agrega as contagens de trabalhos para todos os estados e retorna a soma.

Valores Válidos: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AggregationPeriod

O período para os resultados retornados.

- `ONE_DAY`- A contagem diária de trabalhos dos 14 dias anteriores.
- `SEVEN_DAYS`- A contagem agregada de trabalhos dos 7 dias anteriores.
- `FOURTEEN_DAYS`- A contagem agregada de empregos dos 14 dias anteriores.

Tipo: sequência

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `MaxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

RestoreJobSummaries

Essa devolução contém um resumo que contém região, conta, estado ResourceType, MessageCategory, StartTime, EndTime, e contagem de trabalhos incluídos.

Tipo: matriz de objetos RestoreJobSummary

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma lista de planos de testes de restauração.

Sintaxe da Solicitação

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar a quantidade `MaxResults` de itens, `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar a quantidade `MaxResults` de itens, `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

RestoreTestingPlans

Essa é uma lista retornada de planos de testes de restauração.

Tipo: matriz de objetos RestoreTestingPlanForList

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna uma lista de seleções de testes de restauração. Pode ser filtrada por `MaxResults` e `RestoreTestingPlanName`.

Sintaxe da Solicitação

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar a quantidade `MaxResults` de itens, `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

RestoreTestingPlanName

Retorna as seleções de testes de restauração pelo nome do plano de testes de restauração especificado.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar a quantidade `MaxResults` de itens, `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

RestoreTestingSelections

Retorna as seleções de testes de restauração associadas ao plano de testes de restauração.

Tipo: matriz de objetos RestoreTestingSelectionForList

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Retorna as tags atribuídas ao recurso, como um ponto de recuperação de destino, um plano de backup ou um cofre de backup.

`ListTags` só funciona para tipos de recursos compatíveis com gerenciamento completo do AWS Backup de seus backups. Esses tipos de recursos estão listados na tabela Disponibilidade de recursos por recurso.

Sintaxe da Solicitação

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

MaxResults

O número máximo de itens a serem retornados.

Intervalo válido: valor mínimo de 1. Valor máximo de 1.000.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

resourceArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso. Os destinos válidos para `ListTags` são pontos de recuperação, planos de backup e cofres de backup.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos itens retornados. Por exemplo, se for feita uma solicitação para retornar o número `MaxResults` de itens, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Tags

Informações sobre as tags.

Tipo: mapa de string para string

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Define uma política baseada em recurso usada para gerenciar as permissões de acesso ao cofre de backup de destino. Requer um nome de cofre de backup e um documento de política de acesso no formato JSON.

Sintaxe da Solicitação

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

Policy

O documento da política de acesso ao cofre de backup no formato JSON.

Tipo: sequência

Obrigatório: não

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Aplica o AWS Backup Vault Lock a um cofre de backup, evitando tentativas de excluir qualquer ponto de recuperação armazenado ou criado em um cofre de backup. O Vault Lock também impede tentativas de atualizar a política de ciclo de vida que controla o período de retenção de qualquer ponto de recuperação atualmente armazenado em um cofre de backup. Se especificado, o Vault Lock impõe um período mínimo e máximo de retenção para futuros trabalhos de backup e de cópia destinados a um cofre de backup.

> **Note**
>
> AWS Backup O Vault Lock foi avaliado pela Cohasset Associates para uso em ambientes sujeitos às regulamentações SEC 17a-4, CFTC e FINRA. Para obter mais informações sobre como o AWS Backup Vault Lock se relaciona com esses regulamentos, consulte a Avaliação de conformidade da Cohasset Associates.

Para obter mais informações, consulte Vault Lock do AWS Backup.

Sintaxe da Solicitação

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

A configuração do AWS Backup Vault Lock que especifica o nome do cofre de backup que ele protege.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

ChangeableForDays

A configuração do AWS Backup Vault Lock que especifica o número de dias antes da data do bloqueio. Por exemplo, definindo `ChangeableForDays` para 30 em 1º de janeiro de 2022 às 20h UTC definirá a data de bloqueio para 31 de janeiro de 2022 às 20h UTC.

AWS Backup impõe um período de reflexão de 72 horas antes que o Vault Lock entre em vigor e se torne imutável. Portanto, você deve definir o `ChangeableForDays` para 3 ou mais.

Antes da data de bloqueio, você pode excluir o Vault Lock do cofre usando`DeleteBackupVaultLockConfiguration` ou alterar a configuração do Vault Lock usando `PutBackupVaultLockConfiguration`. Na data de bloqueio e após essa data, o Vault Lock se tornará imutável e não poderá ser alterado ou excluído.

Se esse parâmetro não for especificado, você poderá excluir o Vault Lock do cofre usando `DeleteBackupVaultLockConfiguration` ou alterar a configuração do Vault Lock usando `PutBackupVaultLockConfiguration` a qualquer momento.

Tipo: longo

Obrigatório: não

MaxRetentionDays

A configuração do AWS Backup Vault Lock que especifica o período máximo de retenção em que o cofre retém seus pontos de recuperação. Essa configuração pode ser útil se, por exemplo, as políticas da sua organização exigirem que você destrua determinados dados depois de retê-los por quatro anos (1460 dias).

Se esse parâmetro não estiver incluído, o Vault Lock não aplicará um período máximo de retenção nos pontos de recuperação no cofre. Se esse parâmetro for incluído sem um valor, o Vault Lock não aplicará um período máximo de retenção.

Se esse parâmetro for especificado, qualquer tarefa de backup ou cópia para o cofre deverá ter uma política de ciclo de vida com um período de retenção igual ou inferior ao período máximo de

retenção. Se o período de retenção do trabalho for maior do que o período máximo de retenção, o cofre falhará no trabalho de backup ou cópia e você deverá modificar as configurações do ciclo de vida ou usar um cofre diferente. O período máximo de retenção mais longo que pode ser especificado é de 36.500 dias (aproximadamente 100 anos). Os pontos de recuperação já salvos no cofre antes do Vault Lock não serão afetados.

Tipo: longo

Obrigatório: não

MinRetentionDays

A configuração do AWS Backup Vault Lock que especifica o período mínimo de retenção em que o cofre retém seus pontos de recuperação. Essa configuração pode ser útil se, por exemplo, as políticas da sua organização exigirem que você retenha determinados dados por pelo menos sete anos (2555 dias).

Esse parâmetro é necessário quando um bloqueio de cofre é criado por meio de AWS CloudFormation; caso contrário, esse parâmetro é opcional. Se esse parâmetro não for especificado, o Vault Lock não aplicará um período mínimo de retenção.

Se esse parâmetro for especificado, qualquer tarefa de backup ou cópia para o cofre deverá ter uma política de ciclo de vida com um período de retenção igual ou superior ao período mínimo de retenção. Se o período de retenção do trabalho for mais curto do que o período mínimo de retenção, o cofre falhará no trabalho de backup ou cópia e você deverá modificar as configurações do ciclo de vida ou usar um cofre diferente. O período mínimo de retenção mais curto que você ser especificado é de 1 dia. Os pontos de recuperação já salvos no cofre antes do Vault Lock não serão afetados.

Tipo: longo

Obrigatório: Não

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Ativa as notificações em um cofre de backup para o tópico e os eventos especificados.

Sintaxe da Solicitação

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

BackupVaultEvents

Uma matriz de eventos que indicam o status de trabalhos para recursos de backup para o cofre de backup.

Para casos de uso comuns e exemplos de código, consulte Uso do Amazon SNS para rastrear AWS Backup eventos.

Os seguintes eventos são compatíveis:

- 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**
>
> A lista abaixo inclui eventos compatíveis e eventos obsoletos que não estão mais em uso (para referência). Eventos obsoletos não retornam status ou notificações. Consulte a lista acima para ver os eventos suportados.

Tipo: matriz de strings

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`

Obrigatório: Sim

SNSTopicArn

O Nome do recurso da Amazon (ARN) que especifica o tópico dos eventos de um cofre de backup. Por exemplo, `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Tipo: string

Obrigatório: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Essa solicitação permite que você envie os resultados de validação do teste de restauração de execução própria e independente. `RestoreJobId` e `ValidationStatus` são obrigatórios. Você também pode inserir um `ValidationStatusMessage`.

Sintaxe da Solicitação

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

restoreJobId

Esse é um identificador exclusivo de um trabalho de restauração interno AWS Backup.

Obrigatório: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

ValidationStatus

O status da validação da sua restauração.

Tipo: sequências

Valores Válidos: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Obrigatório: Sim

ValidationStatusMessage

Essa é uma string de mensagem opcional que você pode inserir para descrever o status da validação do teste de restauração.

Tipo: sequência

Obrigatório: não

Sintaxe da Resposta

```
HTTP/1.1 204
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 204 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Iniciar um trabalho de backup sob demanda para o recurso especificado.

Sintaxe da Solicitação

```
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
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

BackupOptions

A opção de backup para um recurso selecionado. Essa opção só está disponível para trabalhos de backup do Serviço de Cópias de Sombra de Volume (VSS) do Windows.

Valores válidos: defina como `"WindowsVSS":"enabled"` para habilitar a opção de backup do `WindowsVSS` e criar um backup do VSS do Windows. Defina `"WindowsVSS""disabled"` como para criar um backup regular. A opção `WindowsVSS` é habilitada por padrão.

Tipo: mapa de string para string

Padrão da chave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Padrão de valor: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: não

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

CompleteWindowMinutes

Um valor em minutos durante o qual um backup iniciado com êxito deve ser concluído, ou então o AWS Backup cancelará o trabalho. Este valor é opcional. Esse valor começa a contagem regressiva a partir do momento em que o backup foi programado. Isso não adiciona tempo adicional para `StartWindowMinutes` ou, se o backup foi iniciado depois do programado.

Como `StartWindowMinutes`, esse parâmetro tem um valor máximo de 100 anos (52.560.000 minutos).

Tipo: longo

Obrigatório: não

IamRoleArn

Especifica o ARN do perfil do IAM usado para criar o ponto de recuperação de destino. Por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: string

Obrigatório: Sim

IdempotencyToken

Uma string escolhida pelo cliente que pode ser usada para distinguir entre chamadas idênticas a `StartBackupJob`. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

Lifecycle

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento refrigerado e quando ele expira. AWS Backup fará a transição e expirará os backups automaticamente de acordo com o ciclo de vida que você definir.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias a mais do que a configuração de “número de dias para a transição para o armazenamento frio”. A configuração de "número de dias para transferência ao armazenamento 'frio'" não poderá ser alterada depois que um backup for transferido para o armazenamento "frio".

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Esse parâmetro tem um valor máximo de 100 anos (36.500 dias).

Tipo: objeto Lifecycle

Obrigatório: Não

RecoveryPointTags

As tags a serem atribuídas aos recursos.

Tipo: mapa de string para string

Obrigatório: não

ResourceArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: string

Obrigatório: Sim

StartWindowMinutes

Um valor em minutos após a programação de um backup antes que um trabalho seja cancelado, se ele não for iniciado com êxito. Esse valor é opcional e o padrão é oito horas. Se esse valor for incluído, deve ser de pelo menos 60 minutos para evitar erros.

Esse parâmetro tem um valor máximo de 100 anos (52.560.000 minutos).

Durante a janela inicial, o status do trabalho de backup permanece no status `CREATED` até que seja iniciado com êxito ou até que o tempo da janela inicial se esgote. Se, dentro da janela inicial, o horário AWS Backup receber um erro que permita que o trabalho seja repetido, AWS Backup tentará iniciá-lo automaticamente pelo menos a cada 10 minutos até que o backup seja iniciado com sucesso (o status do trabalho mude para`RUNNING`) ou até que o status do trabalho mude para `EXPIRED` (o que se espera que ocorra quando o tempo da janela inicial terminar).

Tipo: longo

Obrigatório: Não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupJobId

Identifica de forma exclusiva uma solicitação para AWS Backup fazer backup de um recurso.

Tipo: sequência

CreationDate

A data e a hora em que um trabalho de backup foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

IsParent

Isso é um valor booliano que indica que se trata de um trabalho de backup pai (composto).

Tipo: booliano

RecoveryPointArn

Observação: esse campo só é retornado para recursos do Amazon EFS e do Advanced DynamoDB.

Um ARN que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Inicia um trabalho para criar uma cópia única do recurso especificado.

Essa operação não é compatível com backups contínuos.

Sintaxe da Solicitação

```
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"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

DestinationBackupVaultArn

Um nome de recurso da Amazon (ARN) que identifica de forma exclusiva um cofre de backup de destino. Por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: string

Obrigatório: Sim

IamRoleArn

Especifica o ARN do perfil do IAM usado para copiar o ponto de recuperação de destino. Por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: string

Obrigatório: Sim

IdempotencyToken

Uma string escolhida pelo cliente que pode ser usada para distinguir entre chamadas idênticas a `StartCopyJob`. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

Lifecycle

Especifica o período de tempo, em dias, antes que um ponto de recuperação faça a transição para o armazenamento refrigerado ou seja excluído.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, no console, a configuração de retenção deve ser 90 dias maior do que a configuração de transição para frio após dias. A configuração de transição para frio após dias não pode ser alterada após a transição de um backup para frio.

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Para remover o ciclo de vida e os períodos de retenção existentes e manter seus pontos de recuperação indefinidamente, especifique -1 para e. `MoveToColdStorageAfterDays` `DeleteAfterDays`

Tipo: objeto Lifecycle

Obrigatório: Não

RecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação a ser usado no trabalho de cópia. Por exemplo, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Tipo: string

Obrigatório: Sim

SourceBackupVaultName

O nome de um contêiner lógico de origem em que os backups são armazenados. Os cofres de backup são identificados por nomes exclusivos da conta usada para criá-los e da AWS região em que foram criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CopyJobId

Identifica de forma exclusiva um trabalho de cópia.

Tipo: sequência

CreationDate

A data e a hora em que um trabalho de cópia foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

IsParent

Isso um valor booliano retornado que indica que se trata de um trabalho de cópia pai (composto).

Tipo: booliano

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Inicia um trabalho de relatório sob demanda para o plano de relatório especificado.

Sintaxe da Solicitação

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

reportPlanName

O nome exclusivo de um plano de relatório.

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Exigido: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

IdempotencyToken

Uma string escolhida pelo cliente que pode ser usada para distinguir entre chamadas idênticas para `StartReportJobInput`. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

ReportJobId

O identificador do trabalho de relatório. Uma string Unicode exclusiva, gerada aleatoriamente, codificada em UTF-8, com, no máximo, 1.024 bytes. Não é possível editar o ID do trabalho de relatório.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Recupera o recurso salvo identificado por um Nome do recurso da Amazon (ARN).

Sintaxe da Solicitação

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

CopySourceTagsToRestoredResource

Esse parâmetro é opcional. Se isso for igual a `True`, as tags incluídas no backup serão copiadas para o recurso restaurado.

Isso só pode ser aplicado aos backups criados por meio de AWS Backup.

Tipo: booliano

Obrigatório: não

IamRoleArn

O Amazon Resource Name (ARN) da função do IAM AWS Backup usada para criar o recurso de destino; por exemplo:. `arn:aws:iam::123456789012:role/S3Access`

Tipo: sequência

Obrigatório: não

IdempotencyToken

Uma string escolhida pelo cliente que você pode usar para distinguir entre chamadas idênticas para `StartRestoreJob`. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

Metadata

Um conjunto de pares de chave/valor de metadados.

É possível obter metadados de configuração sobre um recurso no momento em que o backup foi feito por meio de uma chamada a `GetRecoveryPointRestoreMetadata`. No entanto, valores além dos fornecidos por `GetRecoveryPointRestoreMetadata` podem ser necessários para restaurar um recurso. Por exemplo, talvez seja necessário fornecer um novo nome de recurso caso o original já exista.

Para obter mais informações sobre os metadados de cada recurso, consulte o seguinte:

- Metadados para Amazon Aurora
- Metadados para Amazon DocumentDB
- Metadados para AWS CloudFormation
- Metadados para o Amazon DynamoDB
- Metadados para Amazon EBS
- Metadados para o Amazon EC2
- Metadados para Amazon EFS
- Metadados para Amazon FSx
- Metadados para o Amazon Neptune
- Metadados para Amazon RDS
- Metadados para o Amazon Redshift
- Metadados para AWS Storage Gateway
- Metadados para o Amazon S3

- Metadados para Amazon Timestream
- Metadados para máquinas virtuais

Tipo: mapa de string para string

Obrigatório: Sim

RecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: string

Obrigatório: Sim

ResourceType

Inicia um trabalho para restaurar um ponto de recuperação para um dos seguintes recursos:

- `Aurora`- Amazon Aurora
- `DocumentDB`- Amazon DocumentDB
- `CloudFormation` - AWS CloudFormation
- `DynamoDB`- Amazon DynamoDB
- `EBS`- Amazon Elastic Block Store
- `EC2`- Nuvem de computação elástica da Amazon
- `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`- Serviço Amazon Simple Storage
- `Timestream`- Amazon Timestream
- `VirtualMachine`- Máquinas virtuais

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: Não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

RestoreJobId

Identifica de forma exclusiva o trabalho que restaura um ponto de recuperação.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Tenta cancelar um trabalho para criar um backup único de um recurso.

Essa ação não é compatível com os seguintes serviços: Amazon FSx para Windows File Server, Amazon FSx for Lustre, Amazon FSx for ONTAP, Amazon NetApp FSx for OpenZFS, Amazon DocumentDB (com compatibilidade com MongoDB), Amazon RDS, Amazon Aurora e Amazon Neptune ptune.

Sintaxe da Solicitação

```
POST /backup-jobs/backupJobId HTTP/1.1
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupJobId

Identifica de forma exclusiva uma solicitação para AWS Backup fazer backup de um recurso.

Obrigatório: Sim

Corpo da Solicitação

Essa solicitação não tem corpo.

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Atribui um conjunto de pares de chave/valor a um ponto de recuperação, plano de backup ou cofre de backup identificado por um Nome do recurso da Amazon (ARN).

Essa API é compatível com pontos de recuperação para tipos de recursos, incluindo Aurora e Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune e Amazon RDS.

Sintaxe da Solicitação

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

resourceArn

Um ARN identifica de forma exclusiva um recurso. O formato do ARN depende do tipo do recurso marcado.

Os ARNs que não incluem `backup` são incompatíveis com a marcação. `TagResource`e `UntagResource` com ARNs inválidos resultará em um erro. O conteúdo ARN aceitável pode incluir. `arn:aws:backup:us-east` O conteúdo de ARN inválido pode parecer assim. `arn:aws:ec2:us-east`

Obrigatório: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

Tags

Os pares de chave/valor que são usados para ajudar a organizar seus recursos. É possível atribuir seus próprios metadados aos recursos que você criar. Para maior clareza, esta é a estrutura para atribuir tags: `[{"Key":"string","Value":"string"}]`.

Tipo: mapa de string para string

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Remove um conjunto de pares de chave/valor de um ponto de recuperação, plano de backup ou cofre de backup identificado por um Nome do recurso da Amazon (ARN)

Essa API não é compatível com pontos de recuperação de tipos de recursos, incluindo Aurora e Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune e Amazon RDS.

Sintaxe da Solicitação

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

resourceArn

Um ARN identifica de forma exclusiva um recurso. O formato do ARN depende do tipo do recurso marcado.

Os ARNs que não incluem `backup` são incompatíveis com a marcação. `TagResource`e `UntagResource` com ARNs inválidos resultará em um erro. O conteúdo ARN aceitável pode incluir. `arn:aws:backup:us-east` O conteúdo de ARN inválido pode parecer assim. `arn:aws:ec2:us-east`

Obrigatório: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

TagKeyList

As chaves para identificar quais tags de valor-chave devem ser removidas de um recurso.

Tipo: matriz de strings

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Atualiza o plano de backup especificado. A nova versão é identificada exclusivamente por seu ID.

Sintaxe da Solicitação

```
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"
         }
      ]
   }
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupPlanId

O ID do plano de backup.

Obrigatório: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

BackupPlan

O corpo de um plano alternativo. Inclui um `BackupPlanName` e um ou mais conjuntos de `Rules`.

Tipo: objeto BackupPlanInput

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
```

```
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AdvancedBackupSettings

Contém uma lista de `BackupOptions` para cada tipo de recurso.

Tipo: matriz de objetos AdvancedBackupSetting

BackupPlanArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um plano de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: sequência

BackupPlanId

Identifica exclusivamente um plano de backup.

Tipo: sequência

CreationDate

A data e hora em que um plano de backup foi criada, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

VersionId

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. IDs de versão não podem ser editados.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Atualiza a estrutura especificada.

Sintaxe da Solicitação

```
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"
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

frameworkName

O nome exclusivo de uma framework. Esse nome tem entre 1 e 256 caracteres, começando com uma letra, e consiste em letras (a-z, A-Z), números (0-9) e sublinhados (_).

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Exigido: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

FrameworkControls

Os controles que compõem a estrutura. Cada controle na lista tem um nome, parâmetros de entrada e escopo.

Tipo: matriz de objetos FrameworkControl

Obrigatório: não

FrameworkDescription

Uma descrição opcional da framework com no máximo 1.024 caracteres.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 1.024.

Padrão: `.*\S.*`

Obrigatório: não

IdempotencyToken

Uma string escolhida pelo cliente que você pode usar para distinguir entre chamadas idênticas para `UpdateFrameworkInput`. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "CreationTime": number,
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A data e a hora em que a framework é criada, na representação ISO 8601. O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, 2020-07-10T15:00:00.000-08:00 representa o dia 10 de julho de 2020 às 15:00, 8 horas antes do UTC.

Tipo: carimbo de data/hora

FrameworkArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

FrameworkName

O nome exclusivo de uma framework. Esse nome tem entre 1 e 256 caracteres, começando com uma letra, e consiste em letras (a-z, A-Z), números (0-9) e sublinhados (_).

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AlreadyExistsException

O recurso necessário já existe.

Código de Status HTTP: 400

ConflictException

AWS Backup não pode realizar a ação que você solicitou até que ela termine de executar uma ação anterior. Tente novamente mais tarde.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, o número máximo de itens permitidos em uma solicitação.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Atualiza se a AWS conta optou por fazer backup entre contas. Retorna um erro se a conta não for uma conta de gerenciamento do Organizations. Use a API `DescribeGlobalSettings` para determinar as configurações atuais.

Sintaxe da Solicitação

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

GlobalSettings

Um valor para `isCrossAccountBackupEnabled` e uma região. Exemplo: `update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

Tipo: mapa de string para string

Obrigatório: Não

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Define o ciclo de vida de transição de um ponto de recuperação.

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento refrigerado e quando ele expira. AWS Backup faz a transição e expira os backups automaticamente de acordo com o ciclo de vida definido por você.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias a mais do que a configuração de “número de dias para a transição para o armazenamento frio”. A configuração de "número de dias para transferência ao armazenamento 'frio'" não poderá ser alterada depois que um backup for transferido para o armazenamento "frio".

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Essa operação não é compatível com backups contínuos.

Sintaxe da Solicitação

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

backupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

recoveryPointArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obrigatório: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

Lifecycle

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento refrigerado e quando ele expira. AWS Backup faz a transição e expira os backups automaticamente de acordo com o ciclo de vida definido por você.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias a mais do que a configuração de “número de dias para a transição para o armazenamento frio”. A configuração de "número de dias para transferência ao armazenamento 'frio'" não poderá ser alterada depois que um backup for transferido para o armazenamento "frio".

Tipo: objeto Lifecycle

Obrigatório: Não

Sintaxe da Resposta

```
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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BackupVaultArn

Um ARN que identifica de forma exclusiva um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

CalculatedLifecycle

Um objeto `CalculatedLifecycle` que contém os timestamps `MoveToColdStorageAt` e `DeleteAt`.

Tipo: objeto CalculatedLifecycle

Lifecycle

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento refrigerado e quando ele expira. AWS Backup faz a transição e expira os backups automaticamente de acordo com o ciclo de vida definido por você.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias a mais do que a configuração de

"número de dias para a transição para o armazenamento frio". A configuração de "número de dias para transferência ao armazenamento 'frio'" não poderá ser alterada depois que um backup for transferido para o armazenamento "frio".

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Tipo: objeto Lifecycle

RecoveryPointArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um ponto de recuperação, por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

InvalidRequestException

Indica que há algo errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Atualiza as configurações atuais de inclusão do serviço para a região.

Use a API `DescribeRegionSettings` para determinar os tipos de recursos compatíveis.

Sintaxe da Solicitação

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

ResourceTypeManagementPreference

Ativa ou desativa o AWS Backup gerenciamento completo de backups para um tipo de recurso. Para habilitar o AWS Backup gerenciamento completo do DynamoDB junto com os recursos avançados de backup AWS Backup do DynamoDB, siga o procedimento para habilitar programaticamente o backup avançado do DynamoDB.

Tipo: mapa de string para booliano

Padrão da chave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: não

ResourceTypeOptInPreference

Atualiza a lista de serviços junto com as preferências de inclusão para a região.

Se as atribuições de recursos forem baseadas somente em tags, as configurações de inclusão do serviço serão aplicadas. Se um tipo de recurso for explicitamente atribuído a um plano de backup, como o Amazon S3, Amazon EC2 ou Amazon RDS, ele será incluído no backup mesmo que a inclusão não esteja habilitada para esse serviço específico. Se o tipo de recurso e as tags forem especificados em uma atribuição de recurso, o tipo de recurso especificado no plano de backup terá prioridade sobre a condição da tag. As configurações de inclusão do serviço serão desconsideradas nessa situação.

Tipo: mapa de string para booliano

Padrão da chave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: Não

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Atualiza o plano de relatório especificado.

Sintaxe da Solicitação

```
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"
   }
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

reportPlanName

O nome exclusivo do plano de relatório. Esse nome tem entre 1 e 256 caracteres, começando com uma letra, e consiste em letras (a-z, A-Z), números (0-9) e sublinhados (_).

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Exigido: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

IdempotencyToken

Uma string escolhida pelo cliente que pode ser usada para distinguir entre chamadas idênticas para `UpdateReportPlanInput`. Tentar novamente uma solicitação com êxito com o mesmo token de idempotência resultará em uma mensagem de êxito sem nenhuma ação tomada.

Tipo: string

Obrigatório: não

ReportDeliveryChannel

As informações sobre onde entregar seus relatórios, especificamente o nome do bucket do Amazon S3, o prefixo da chave do S3 e os formatos dos seus relatórios.

Tipo: objeto ReportDeliveryChannel

Obrigatório: Não

ReportPlanDescription

Uma descrição opcional do plano de relatório com no máximo 1.024 caracteres.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 1.024.

Padrão: `.*\S.*`

Obrigatório: não

ReportSetting

O modelo de relatório para o relatório. Relatórios são criados utilizando um modelo de relatório. Os modelos de relatório são:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Se o modelo de relatório for `RESOURCE_COMPLIANCE_REPORT` ou`CONTROL_COMPLIANCE_REPORT`, esse recurso de API também descreve a cobertura do relatório por Regiões da AWS estruturas.

Tipo: objeto ReportSetting

Obrigatório: Não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A data e hora em que um plano de relatório foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

ReportPlanArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

ReportPlanName

O nome exclusivo do plano de relatório.

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

AWS Backup não pode realizar a ação que você solicitou até que termine de executar uma ação anterior. Tente novamente mais tarde.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface

- 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

Serviço: AWS Backup

Essa solicitação enviará alterações ao plano de testes de restauração especificado. `RestoreTestingPlanName` não pode ser atualizado após a criação.

`RecoveryPointSelection` pode conter:

- `Algorithm`
- `ExcludeVaults`
- `IncludeVaults`
- `RecoveryPointTypes`
- `SelectionWindowDays`

Sintaxe da Solicitação

```
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
   }
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

RestoreTestingPlanName

O nome do plano de teste de restauração.

Obrigatório: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

RestoreTestingPlan

Especifica o corpo de um plano de testes de restauração.

Tipo: objeto RestoreTestingPlanForUpdate

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A hora em que o plano de teste de recursos foi criado.

Tipo: carimbo de data/hora

RestoreTestingPlanArn

ARN (nome do recurso da Amazon) exclusivo do plano de testes de restauração.

Tipo: sequência

RestoreTestingPlanName

O nome não poderá ser alterado após a criação. Ele só pode conter caracteres alfanuméricos e sublinhados. O tamanho máximo é 50.

Tipo: sequência

UpdateTime

A hora em que a atualização foi concluída para o plano de teste de restauração.

Tipo: carimbo de data/hora

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

AWS Backup não pode realizar a ação que você solicitou até que termine de executar uma ação anterior. Tente novamente mais tarde.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup

Atualiza a seleção de teste de restauração especificada.

A maioria dos elementos, exceto `RestoreTestingSelectionName`, pode ser atualizada com essa solicitação.

Você pode usar ARNs ou condições de recursos protegidos, mas não ambos.

Sintaxe da Solicitação

```
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
   }
}
```

Parâmetros da Solicitação de URI

A solicitação usa os seguintes parâmetros de URI:

RestoreTestingPlanName

O nome do plano de testes de restauração é necessário para atualizar o plano de testes indicado.

Obrigatório: Sim

RestoreTestingSelectionName

O nome da seleção de teste de restauração necessária da seleção de teste de restauração que você deseja atualizar.

Obrigatório: Sim

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

RestoreTestingSelection

Para atualizar uma seleção de testes de restauração, você pode usar ARNs de recursos protegidos ou condições, mas não ambos. Ou seja, se a sua seleção tiver `ProtectedResourceArns`, a solicitação de uma atualização com o parâmetro `ProtectedResourceConditions` não será bem-sucedida.

Tipo: objeto RestoreTestingSelectionForUpdate

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
```

```
    "RestoreTestingSelectionName": "string",
    "UpdateTime": number
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A hora em que a seleção do teste de recursos foi atualizada com êxito.

Tipo: carimbo de data/hora

RestoreTestingPlanArn

Essa string exclusiva é o nome do plano de testes de restauração.

Tipo: sequência

RestoreTestingPlanName

O plano de teste de restauração ao qual a seleção de teste de restauração atualizada está associada.

Tipo: sequência

RestoreTestingSelectionName

O nome da seleção do teste de restauração retornado.

Tipo: sequência

UpdateTime

A hora em que a atualização foi concluída para a seleção do teste de restauração.

Tipo: carimbo de data/hora

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

AWS Backup não pode realizar a ação que você solicitou até que ela termine de executar uma ação anterior. Tente novamente mais tarde.

Código de Status HTTP: 400

InvalidParameterValueException

Indica que há algo errado com o valor de um parâmetro. Por exemplo, o valor está fora do intervalo.

Código de Status HTTP: 400

MissingParameterValueException

Indica que um parâmetro necessário está ausente.

Código de Status HTTP: 400

ResourceNotFoundException

Um recurso necessário para a ação não existe.

Código de Status HTTP: 400

ServiceUnavailableException

Houve falha na solicitação devido a um erro temporário do servidor.

Código de Status HTTP: 500

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

As seguintes ações são compatíveis com o AWS Backup gateway:

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines
- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow

- UpdateHypervisor

AssociateGatewayToServer

Serviço: AWS Backup gateway

Associa um gateway de backup ao seu servidor. Depois de concluir o processo de associação, você poderá fazer backup e restaurar suas VMs por meio do gateway.

Sintaxe da Solicitação

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway. Use a `ListGateways` operação para retornar uma lista de gateways para sua conta e. Região da AWS

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

ServerArn

O Nome do recurso da Amazon (ARN) do servidor que hospeda suas máquinas virtuais.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "GatewayArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

Não foi possível continuar a operação porque ela não é compatível.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Cria um gateway de backup. Depois de criar um gateway, você poderá associá-lo a um servidor usando a operação `AssociateGatewayToServer`.

Sintaxe da Solicitação

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

ActivationKey

A chave de ativação do gateway criado.

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Tamanho máximo de 50.

Padrão: `^[0-9a-zA-Z\-]+$`

Exigido: Sim

GatewayDisplayName

O nome de exibição do gateway criado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Exigido: Sim

GatewayType

O tipo de gateway criado.

Tipo: sequências

Valores Válidos: `BACKUP_VM`

Obrigatório: Sim

Tags

Uma lista de até 50 tags a serem atribuídas ao gateway. Cada tag é um par de chave/valor.

Tipo: matriz de objetos Tag

Obrigatório: Não

Sintaxe da Resposta

```
{
   "GatewayArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway criado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Exclui um gateway de backup.

Sintaxe da Solicitação

```
{
   "GatewayArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway a ser excluído.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "GatewayArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway excluído.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Exclui um hipervisor.

Sintaxe da Solicitação

```
{
   "HypervisorArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor a ser excluído.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "HypervisorArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor excluído.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AccessDeniedException

Não foi possível continuar a operação porque você não tem permissões suficientes.

Código de Status HTTP: 400

ConflictException

Não foi possível continuar a operação porque ela não é compatível.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Desassocia um gateway de backup do servidor especificado. Depois que o processo de dissociação for concluído, o gateway não poderá mais acessar as máquinas virtuais no servidor.

Sintaxe da Solicitação

```
{
   "GatewayArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

GatewayArn

O nome de recurso da Amazon (ARN) do gateway a ser desassociado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "GatewayArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway desassociado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

Não foi possível continuar a operação porque ela não é compatível.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Recupera a programação dos limites da taxa de largura de banda para um gateway especificado. Por padrão, os gateways não têm programações de limite de taxa de largura de banda, o que significa que nenhum limite de taxa de largura de banda está em vigor. Use isso para obter uma programação de limite de taxa de largura de banda de um gateway.

Sintaxe da Solicitação

```
{
   "GatewayArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway. Use a `ListGateways`operação para retornar uma lista de gateways para sua conta e. Região da AWS

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "BandwidthRateLimitIntervals": [
      {
```

```
            "AverageUploadRateLimitInBitsPerSec": number,
            "DaysOfWeek": [ number ],
            "EndHourOfDay": number,
            "EndMinuteOfHour": number,
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
        }
    ],
    "GatewayArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BandwidthRateLimitIntervals

Uma matriz contendo intervalos de programação de limite de taxa de largura de banda para um gateway. Quando nenhum intervalo limite de taxa de largura de banda é programado, a matriz fica vazia.

Tipo: matriz de objetos BandwidthRateLimitInterval

Membros da Matriz: número mínimo de 0 itens. Número máximo de 20 itens.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway. Use a `ListGateways`operação para retornar uma lista de gateways para sua conta e. Região da AWS

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Ao fornecer o ARN (Nome do recurso da Amazon), essa API retorna o gateway.

Sintaxe da Solicitação

```
{
   "GatewayArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "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 Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Gateway

Ao fornecer o ARN (Nome do recurso da Amazon), essa API retorna o gateway.

Tipo: objeto GatewayDetails

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Essa ação solicita informações sobre o hipervisor especificado ao qual o gateway se conectará. Um hipervisor é um hardware, software ou firmware que cria e gerencia máquinas virtuais e aloca recursos para elas.

Sintaxe da Solicitação

```
{
   "HypervisorArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
      "LatestMetadataSyncStatus": "string",
```

```
      "LatestMetadataSyncStatusMessage": "string",
      "LogGroupArn": "string",
      "Name": "string",
      "State": "string"
   }
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Hypervisor

Detalhes sobre o hipervisor solicitado.

Tipo: objeto HypervisorDetails

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Essa ação recupera os mapeamentos de propriedades do hipervisor especificado. Um mapeamento de propriedades do hipervisor exibe a relação das propriedades da entidade disponíveis no hipervisor com as propriedades disponíveis no. AWS

Sintaxe da Solicitação

```
{
   "HypervisorArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
```

```
            "AwsTagValue": "string",
            "VmwareCategory": "string",
            "VmwareTagName": "string"
        }
    ]
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

O Nome do recurso da Amazon (ARN) do perfil do IAM.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 20. Tamanho máximo de 2.048.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

Essa é uma exibição dos mapeamentos das tags da VMware para as tags da AWS .

Tipo: matriz de objetos VmwareToAwsTagMapping

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Ao fornecer o ARN (Nome do recurso da Amazon), essa API retorna a máquina virtual.

Sintaxe da Solicitação

```
{
   "ResourceArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

ResourceArn

O Nome do recurso da Amazon (ARN) da máquina virtual.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
      "VmwareTags": [
```

```
            {
               "VmwareCategory": "string",
               "VmwareTagDescription": "string",
               "VmwareTagName": "string"
            }
         ]
      }
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

VirtualMachine

Este objeto contém os atributos básicos da `VirtualMachine` contidos na saída da `GetVirtualMachine`

Tipo: objeto VirtualMachineDetails

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Conecte-se a um hipervisor importando sua configuração.

Sintaxe da Solicitação

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

Host

O host do servidor do hipervisor. Isso pode ser um endereço IP ou um nome de domínio totalmente qualificado (FQDN).

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 3. O tamanho máximo é 128.

Padrão: `^.+$`

Exigido: Sim

KmsKeyArn

O AWS Key Management Service para o hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Obrigatório: não

Name

O nome do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Exigido: Sim

Password

A senha do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[ -~]+$`

Obrigatório: não

Tags

As tags da configuração do hipervisor a ser importada.

Tipo: matriz de objetos Tag

Obrigatório: não

Username

O nome de usuário do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Obrigatório: Não

Sintaxe da Resposta

```
{
   "HypervisorArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor desassociado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AccessDeniedException

Não foi possível continuar a operação porque você não tem permissões suficientes.

Código de Status HTTP: 400

ConflictException

Não foi possível continuar a operação porque ela não é compatível.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Lista os gateways de backup pertencentes a um Conta da AWS em um Região da AWS. A lista retornada é solicitada pelo Nome do recurso da Amazon (ARN) do gateway.

Sintaxe da Solicitação

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

MaxResults

O número máximo de gateways a serem listados.

Tipo: inteiro

Intervalo válido: valor mínimo de 1.

Obrigatório: não

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `MaxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.000.

Padrão: `^.+$`

Obrigatório: Não

Sintaxe da Resposta

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Gateways

Uma lista dos seus gateways.

Tipo: matriz de objetos Gateway

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `maxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.000.

Padrão: `^.+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Lista seus hipervisores.

Sintaxe da Solicitação

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

MaxResults

O número máximo de hipervisores a serem listados.

Tipo: inteiro

Intervalo válido: valor mínimo de 1.

Obrigatório: não

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `maxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.000.

Padrão: `^.+$`

Obrigatório: Não

Sintaxe da Resposta

```
{
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Hypervisors

Lista seus objetos `Hypervisor`, ordenados por Nomes de recurso da Amazon (ARNs).

Tipo: matriz de objetos Hypervisor

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `maxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.000.

Padrão: `^.+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Lista as tags aplicadas ao recurso identificado pelo seu Nome do recurso da Amazon (ARN).

Sintaxe da Solicitação

```
{
   "ResourceArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

ResourceArn

O Nome do recurso da Amazon (ARN) das tags do recurso a serem listadas.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
```

```
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

ResourceArn

O Nome do recurso da Amazon (ARN) das tags do recurso que você listou.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

Listar as tags do recurso.

Tipo: matriz de objetos Tag

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Lista suas máquinas virtuais.

Sintaxe da Solicitação

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor conectado à sua máquina virtual.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obrigatório: não

MaxResults

O número máximo de máquinas virtuais a serem listadas.

Tipo: inteiro

Intervalo válido: valor mínimo de 1.

Obrigatório: não

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `maxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.000.

Padrão: `^.+$`

Obrigatório: Não

Sintaxe da Resposta

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

O próximo item após uma lista parcial dos recursos retornados. Por exemplo, se uma solicitação for feita para retornar o número `maxResults` de recursos, o `NextToken` permitirá que você retorne mais itens em sua lista começando pelo local apontado pelo próximo token.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.000.

Padrão: `^.+$`

VirtualMachines

Uma lista de seus objetos `VirtualMachine`, ordenada por Nomes de recursos da Amazon (ARNs).

Tipo: matriz de objetos VirtualMachine

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Essa ação define a programação dos limites da taxa de largura de banda para um gateway especificado. Por padrão, os gateways não têm uma programação de limite de taxa de largura de banda, o que significa que nenhum limite de taxa de largura de banda está em vigor. Use isso para iniciar a programação de limite de taxa de largura de banda de um gateway.

Sintaxe da Solicitação

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

BandwidthRateLimitIntervals

Uma matriz contendo intervalos de programação de limite de taxa de largura de banda para um gateway. Quando nenhum intervalo limite de taxa de largura de banda é programado, a matriz fica vazia.

Tipo: matriz de objetos BandwidthRateLimitInterval

Membros da Matriz: número mínimo de 0 itens. Número máximo de 20 itens.

Obrigatório: Sim

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway. Use a `ListGateways`operação para retornar uma lista de gateways para sua conta e. Região da AWS

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "GatewayArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway. Use a `ListGateways`operação para retornar uma lista de gateways para sua conta e. Região da AWS

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Essa ação define os mapeamentos de propriedades para o hipervisor especificado. Um mapeamento de propriedades do hipervisor exibe a relação das propriedades da entidade disponíveis no hipervisor com as propriedades disponíveis no. AWS

Sintaxe da Solicitação

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

IamRoleArn

O Nome do recurso da Amazon (ARN) do perfil do IAM.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 20. Tamanho máximo de 2.048.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

Exigido: Sim

VmwareToAwsTagMappings

Essa ação solicita o mapeamento das tags da VMware para as tags da AWS .

Tipo: matriz de objetos VmwareToAwsTagMapping

Exigido: Sim

Sintaxe da Resposta

```
{
   "HypervisorArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AccessDeniedException

Não foi possível continuar a operação porque você não tem permissões suficientes.

Código de Status HTTP: 400

ConflictException

Não foi possível continuar a operação porque ela não é compatível.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Defina o horário de início da manutenção de um gateway.

Sintaxe da Solicitação

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

DayOfMonth

O dia do mês para iniciar a manutenção em um gateway.

Os valores válidos variam de `Sunday` até `Saturday`.

Tipo: inteiro

Intervalo válido: valor mínimo de 1. Valor máximo de 31.

Obrigatório: não

DayOfWeek

O dia da semana para iniciar a manutenção em um gateway.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 6.

Obrigatório: não

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway, usado para especificar o horário de início da manutenção.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

HourOfDay

A hora do dia para iniciar a manutenção em um gateway.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 23.

Obrigatório: Sim

MinuteOfHour

O minuto da hora para iniciar a manutenção em um gateway.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 59.

Exigido: Sim

Sintaxe da Resposta

```
{
   "GatewayArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

GatewayArn

O Nome do recurso da Amazon (ARN) de um gateway para o qual você define o horário de início da manutenção.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

Não foi possível continuar a operação porque ela não é compatível.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Essa ação envia uma solicitação para sincronizar metadados nas máquinas virtuais especificadas.

Sintaxe da Solicitação

```
{
   "HypervisorArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "HypervisorArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AccessDeniedException

Não foi possível continuar a operação porque você não tem permissões suficientes.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Marca o recurso.

Sintaxe da Solicitação

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

ResourceARN

O Nome do recurso da Amazon (ARN) do recurso a ser marcado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Tags

A lista de tags a serem atribuídas ao recurso.

Tipo: matriz de objetos Tag

Exigido: Sim

Sintaxe da Resposta

```
{
   "ResourceARN": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

ResourceARN

O Nome do recurso da Amazon (ARN) do recurso marcado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Testa a configuração do hipervisor para validar se o gateway de backup pode se conectar ao hipervisor e seus recursos.

Sintaxe da Solicitação

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway para o hipervisor a ser testado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Host

O host do servidor do hipervisor. Isso pode ser um endereço IP ou um nome de domínio totalmente qualificado (FQDN).

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 3. O tamanho máximo é 128.

Padrão: `^.+$`

Exigido: Sim

Password

A senha do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[ -~]+$`

Obrigatório: não

Username

O nome de usuário do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Obrigatório: Não

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

Não foi possível continuar a operação porque ela não é compatível.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Remove tags do recurso.

Sintaxe da Solicitação

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

ResourceARN

O Nome do recurso da Amazon (ARN) do recurso do qual remover as tags.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

TagKeys

A lista de chaves de tag especificando quais tags a serem removidas.

Tipo: matriz de strings

Restrições de Tamanho: Tamanho mínimo 1. O tamanho máximo é 128.

Padrão: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Exigido: Sim

Sintaxe da Resposta

```
{
   "ResourceARN": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

ResourceARN

O Nome do recurso da Amazon (ARN) do recurso do qual remover as tags.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Atualiza o nome de um gateway. Especifique o gateway a ser atualizado usando o Nome do recurso da Amazon (ARN) do gateway em sua solicitação.

Sintaxe da Solicitação

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway a ser atualizado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

GatewayDisplayName

O nome de exibição atualizado do gateway.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: Não

Sintaxe da Resposta

```
{
   "GatewayArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway atualizado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

ConflictException

Não foi possível continuar a operação porque ela não é compatível.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Atualiza o software da máquina virtual (VM) do gateway. A solicitação aciona imediatamente a atualização do software.

> **Note**
>
> Ao fazer essa solicitação, você recebe uma resposta de êxito `200 OK` imediatamente. No entanto, pode levar algum tempo até que a atualização seja concluída.

Sintaxe da Solicitação

```
{
   "GatewayArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway a ser atualizado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

Sintaxe da Resposta

```
{
```

```
   "GatewayArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway atualizado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Serviço: AWS Backup gateway

Atualiza os metadados de um hipervisor, incluindo seu host, nome de usuário e senha. Especifique qual hipervisor atualizar usando o Nome do recurso da Amazon (ARN) do hipervisor em sua solicitação.

Sintaxe da Solicitação

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte Parâmetros comuns.

A solicitação aceita os dados a seguir no formato JSON.

Host

O host atualizado do hipervisor. Isso pode ser um endereço IP ou um nome de domínio totalmente qualificado (FQDN).

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 3. O tamanho máximo é 128.

Padrão: ^.+$

Obrigatório: não

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor a ser atualizado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Exigido: Sim

LogGroupArn

O Nome do recurso da Amazon (ARN) do grupo de gateways no log solicitado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 0. Comprimento máximo de 2.048.

Padrão: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Obrigatório: não

Name

O nome atualizado do hipervisor

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: não

Password

A senha atualizada do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[ -~]+$`

Obrigatório: não

Username

O nome de usuário atualizado do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Obrigatório: Não

Sintaxe da Resposta

```
{
   "HypervisorArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor atualizado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AccessDeniedException

Não foi possível continuar a operação porque você não tem permissões suficientes.

Código de Status HTTP: 400

ConflictException

Não foi possível continuar a operação porque ela não é compatível.

Código de Status HTTP: 400

InternalServerException

A operação não teve êxito porque ocorreu um erro interno. Tente novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

Um recurso necessário para a ação não foi encontrado.

Código de Status HTTP: 400

ThrottlingException

O TPS foi limitado para proteger contra altos volumes de solicitações intencionais ou não intencionais.

Código de Status HTTP: 400

ValidationException

A operação não teve êxito porque ocorreu um erro de validação.

Código de Status HTTP: 400

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- 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

Tipos de dados

Os seguintes tipos de dados são compatíveis com o AWS Backup:

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl

- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

Os seguintes tipos de dados são compatíveis com o AWS Backup gateway:

- BandwidthRateLimitInterval

- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

Os seguintes tipos de dados são compatíveis com o AWS Backup:

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter

- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection

- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

AdvancedBackupSetting

Serviço: AWS Backup

As opções de backup para cada tipo de recurso.

Conteúdo

BackupOptions

Especifica a opção de backup para um recurso selecionado. Essa opção só está disponível para trabalhos de backup do VSS do Windows.

Valores válidos:

Defina como `"WindowsVSS":"enabled"` para habilitar a opção de backup do `WindowsVSS` e criar um backup do VSS do Windows.

Defina `"WindowsVSS":"disabled"` como para criar um backup regular. A opção `WindowsVSS` é habilitada por padrão.

Se especificar uma opção inválida, você obterá uma exceção `InvalidParameterValueException`.

Para obter mais informações sobre backups do VSS do Windows, consulte Criar um backup do Windows habilitado para VSS.

Tipo: mapa de string para string

Padrão da chave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Padrão de valor: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: não

ResourceType

Especifica um objeto que contém o tipo de recurso e as opções de backup. O único tipo de recurso compatível são as instâncias do Amazon EC2 com o Serviço de Cópias de Sombra de Volume (VSS) do Windows. Para ver um CloudFormation exemplo, consulte o CloudFormation modelo de amostra para habilitar o Windows VSS no Guia do AWS Backup Usuário.

Valores válidos: `EC2`.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupJob

Serviço: AWS Backup

Contém informações detalhadas sobre um trabalho de backup.

Conteúdo

AccountId

O ID da conta proprietária do trabalho de backup.

Tipo: string

Padrão: `^[0-9]{12}$`

Obrigatório: não

BackupJobId

Identifica de forma exclusiva uma solicitação para AWS Backup fazer backup de um recurso.

Tipo: sequência

Obrigatório: não

BackupOptions

Especifica a opção de backup para um recurso selecionado. Essa opção só está disponível para trabalhos de backup do Serviço de Cópias de Sombra de Volume (VSS) do Windows.

Valores válidos: defina como `"WindowsVSS":"enabled"` para habilitar a opção de backup do `WindowsVSS` e criar um backup do VSS do Windows. Defina `"WindowsVSS":"disabled"` como para criar um backup regular. Se especificar uma opção inválida, você obterá uma exceção `InvalidParameterValueException`.

Tipo: mapa de string para string

Padrão da chave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Padrão de valor: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: não

BackupSizeInBytes

O tamanho de um backup, em bytes.

Tipo: longo

Obrigatório: não

BackupType

Representa o tipo de backup para um trabalho de backup.

Tipo: sequência

Obrigatório: não

BackupVaultArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

Obrigatório: não

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Obrigatório: não

BytesTransferred

O tamanho em bytes transferido para um cofre de backup no momento em que o status do trabalho foi consultado.

Tipo: longo

Obrigatório: não

CompletionDate

A data e a hora em que um trabalho para criar um trabalho de backup foi concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` tem precisão de

milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

CreatedBy

Contém informações de identificação sobre a criação de um trabalho de backup, incluindo `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion`, e `BackupRuleId` do plano de backup usado para criá-lo.

Tipo: objeto RecoveryPointCreator

Obrigatório: Não

CreationDate

A data e a hora em que um trabalho de backup foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

ExpectedCompletionDate

A data e a hora em que um trabalho para fazer backup de recursos foi concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `ExpectedCompletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

IamRoleArn

Especifica o ARN do perfil do IAM usado para criar o ponto de recuperação de destino. Os perfis do IAM que não sejam o perfil padrão devem incluir `AWSBackup` ou `AwsBackup` no nome do perfil. Por exemplo, `arn:aws:iam::123456789012:role/AWSBackupRDSAccess`. Os nomes de perfil sem essas strings não terão permissões para realizar trabalhos de backup.

Tipo: sequência

Obrigatório: não

InitiationDate

A data em que a tarefa de backup foi iniciada.

Tipo: carimbo de data/hora

Obrigatório: não

IsParent

Isso é um valor booliano que indica que se trata de um trabalho de backup pai (composto).

Tipo: booliano

Obrigatório: não

MessageCategory

Esse parâmetro é a contagem de trabalhos para a categoria de mensagem especificada.

Exemplos de strings podem incluir `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `INVALIDPARAMETERS`. Consulte Monitoramento para obter uma lista de MessageCategory sequências de caracteres.

O valor ANY retorna a contagem de todas as categorias de mensagens.

`AGGREGATE_ALL` agrega as contagens de trabalhos de todas as categorias de mensagens e retorna a soma.

Tipo: sequência

Obrigatório: não

ParentJobId

Isso identifica de forma exclusiva uma solicitação ao AWS Backup para fazer backup de um recurso. O retorno será o ID do trabalho pai (composto).

Tipo: sequência

Obrigatório: não

PercentDone

Contém uma porcentagem estimada de conclusão de um trabalho no momento em que o status do trabalho foi consultado.

Tipo: sequência

Obrigatório: não

RecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

Obrigatório: não

ResourceArn

Um ARN identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

Obrigatório: não

ResourceName

O nome não exclusivo do recurso que pertence ao backup especificado.

Tipo: sequência

Obrigatório: não

ResourceType

O tipo de AWS recurso a ser copiado; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS). Para backups do Serviço de Cópias de Sombra de Volume (VSS) do Windows, o único tipo de recurso compatível é o Amazon EC2.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: não

StartBy

Especifica a hora em formato Unix e Tempo Universal Coordenado (UTC) em que um trabalho de backup deve ser iniciado antes de ser cancelado. O valor é calculado adicionando a janela inicial ao horário programado. Portanto, se o horário programado fosse às 18h e a janela inicial fosse 2 horas, o horário `StartBy` seria às 20h na data especificada. O valor de `StartBy` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

State

O estado atual de um trabalho de backup.

Tipo: sequências

Valores Válidos: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

Obrigatório: não

StatusMessage

Uma mensagem detalhada explicando o status do trabalho para fazer backup de um recurso.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

BackupJobSummary

Serviço: AWS Backup

Isso é um resumo dos trabalhos criados ou em execução nos últimos 30 dias.

O resumo retornado pode conter o seguinte: Região, Conta, Estado, RestourceType, MessageCategory, StartTime EndTime, e Contagem de trabalhos incluídos.

Conteúdo

AccountId

O ID da conta à qual os trabalhos no resumo pertencem.

Tipo: string

Padrão: `^[0-9]{12}$`

Obrigatório: não

Count

O valor como um número de trabalhos em um resumo do trabalhos.

Tipo: inteiro

Obrigatório: não

EndTime

O valor do horário de término de um trabalho em formato numérico.

Esse valor é o horário no formato Unix, Tempo Universal Coordenado (UTC), e com precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

MessageCategory

Esse parâmetro é a contagem de trabalhos para a categoria de mensagem especificada.

Exemplos de strings incluem `AccessDenied`, `Success` e `InvalidParameters`. Consulte Monitoramento para obter uma lista de MessageCategory sequências de caracteres.

O valor ANY retorna a contagem de todas as categorias de mensagens.

AGGREGATE_ALL agrega as contagens de trabalhos de todas as categorias de mensagens e retorna a soma.

Tipo: sequência

Obrigatório: não

Region

As AWS regiões dentro do resumo do trabalho.

Tipo: sequência

Obrigatório: não

ResourceType

Esse valor é a contagem de trabalhos para o tipo de recurso especificado. A solicitação GetSupportedResourceTypes retorna strings para os tipos de recurso compatíveis.

Tipo: string

Padrão: ^[a-zA-Z0-9\-_\.]{1,50}$

Obrigatório: não

StartTime

O valor do horário de início de um trabalho em formato numérico.

Esse valor é o horário no formato Unix, Tempo Universal Coordenado (UTC), e com precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

State

Esse valor é a contagem dos trabalhos com o estado especificado.

Tipo: sequências

Valores Válidos: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupPlan

Serviço: AWS Backup

Contém um nome de exibição opcional do plano de backup e uma matriz de objetos `BackupRule`, sendo que cada um especifica uma regra de backup. Cada regra em um plano de backup é uma tarefa programada separada e pode fazer backup de uma seleção diferente de recursos da AWS .

Conteúdo

BackupPlanName

O nome de exibição de um plano de backup. Deve conter de 1 a 50 caracteres alfanuméricos ou '-_.' .

Tipo: string

Obrigatório: Sim

Rules

Uma matriz de objetos `BackupRule`, em que cada um especifica uma tarefa programada que é usada para fazer backup de uma seleção de recursos.

Tipo: matriz de objetos BackupRule

Obrigatório: Sim

AdvancedBackupSettings

Contém uma lista de `BackupOptions` para cada tipo de recurso.

Tipo: matriz de objetos AdvancedBackupSetting

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

BackupPlanInput

Serviço: AWS Backup

Contém um nome de exibição opcional do plano de backup e uma matriz de objetos `BackupRule`, sendo que cada um especifica uma regra de backup. Cada regra em um plano de backup é uma tarefa programada separada.

Conteúdo

BackupPlanName

O nome de exibição de um plano de backup. Deve conter de 1 a 50 caracteres alfanuméricos ou '-_.' .

Tipo: string

Obrigatório: Sim

Rules

Uma matriz de objetos `BackupRule`, em que cada um especifica uma tarefa programada que é usada para fazer backup de uma seleção de recursos.

Tipo: matriz de objetos BackupRuleInput

Obrigatório: Sim

AdvancedBackupSettings

Especifica uma lista de `BackupOptions` para cada tipo de recurso. Essas configurações só estão disponíveis para trabalhos de backup do Serviço de Cópias de Sombra de Volume (VSS) do Windows.

Tipo: matriz de objetos AdvancedBackupSetting

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupPlansListMember

Serviço: AWS Backup

Contém metadados sobre um plano de backup.

Conteúdo

AdvancedBackupSettings

Contém uma lista de `BackupOptions` para um tipo de recurso.

Tipo: matriz de objetos AdvancedBackupSetting

Obrigatório: não

BackupPlanArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um plano de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: sequência

Obrigatório: não

BackupPlanId

Identifica exclusivamente um plano de backup.

Tipo: sequência

Obrigatório: não

BackupPlanName

O nome de exibição de um plano de backup salvo.

Tipo: sequência

Obrigatório: não

CreationDate

A data e a hora em que o plano de backup de um recurso foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

CreatorRequestId

Uma string exclusiva que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Esse parâmetro é opcional.

Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

DeletionDate

A data e a hora em que um plano de backup foi excluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `DeletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

LastExecutionDate

A última vez que esse plano de backup foi executado. A data e a hora devem estar em formato Unix e UTC (Tempo Universal Coordenado). O valor de `LastExecutionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

VersionId

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. IDs de versão não podem ser editados.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupPlanTemplatesListMember

Serviço: AWS Backup

Um objeto que especifica os metadados associados a um modelo de plano de backup.

Conteúdo

BackupPlanTemplateId

Identifica de forma exclusiva um modelo de plano de backup armazenado.

Tipo: sequência

Obrigatório: não

BackupPlanTemplateName

O nome de exibição opcional de um modelo de plano de backup.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupRule

Serviço: AWS Backup

Especifica uma tarefa programada usada para fazer backup de uma seleção de recursos.

Conteúdo

RuleName

Um nome de exibição para uma regra de backup. Deve conter de 1 a 50 caracteres alfanuméricos ou '-_.' .

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Exigido: Sim

TargetBackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

CompletionWindowMinutes

Um valor em minutos após um trabalho de backup ser iniciado com êxito antes que ele seja concluído ou ele será cancelado pelo AWS Backup. Este valor é opcional.

Tipo: longo

Obrigatório: não

CopyActions

Uma matriz de objetos `CopyAction`, que contém os detalhes da operação de cópia.

Tipo: matriz de objetos CopyAction

Obrigatório: não

EnableContinuousBackup

Especifica se AWS Backup cria backups contínuos. Causas verdadeiras AWS Backup para criar backups contínuos capazes de point-in-time restauração (PITR). Causas falsas (ou não especificadas) AWS Backup para criar backups instantâneos.

Tipo: booliano

Obrigatório: não

Lifecycle

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento refrigerado e quando ele expira. AWS Backup faz a transição e expira os backups automaticamente de acordo com o ciclo de vida definido por você.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias a mais do que a configuração de “número de dias para a transição para o armazenamento frio”. A configuração de "número de dias para transferência ao armazenamento 'frio'" não poderá ser alterada depois que um backup for transferido para o armazenamento "frio".

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Tipo: objeto Lifecycle

Obrigatório: Não

RecoveryPointTags

As tags atribuídas aos recursos associados a essa regra quando restauradas do backup.

Tipo: mapa de string para string

Obrigatório: não

RuleId

Identifica de forma exclusiva uma regra usada para programar o backup de uma seleção de recursos.

Tipo: sequência

Obrigatório: não

ScheduleExpression

Uma expressão cron em UTC especificando quando AWS Backup inicia uma tarefa de backup. Para obter mais informações sobre expressões AWS cron, consulte Programar expressões para regras no Guia do usuário do Amazon CloudWatch Events. . Dois exemplos de expressões AWS cron são `15 * ? * * *` (faça um backup a cada hora, 15 minutos após a hora) e `0 12 * * ? *` (faça um backup todos os dias às 12h UTC). Para ver uma tabela de exemplos, clique no link anterior e role a página para baixo.

Tipo: sequência

Obrigatório: não

ScheduleExpressionTimezone

O fuso horário no qual a expressão do cronograma está definida. Por padrão, ScheduleExpressions estão em UTC. É possível modificar isso para um fuso horário específico.

Tipo: sequência

Obrigatório: não

StartWindowMinutes

Um valor em minutos após a programação de um backup antes que um trabalho seja cancelado, se ele não for iniciado com êxito. Este valor é opcional. Se esse valor for incluído, deve ser de pelo menos 60 minutos para evitar erros.

Durante a janela inicial, o status do trabalho de backup permanece no status `CREATED` até que seja iniciado com êxito ou até que o tempo da janela inicial se esgote. Se, dentro da janela inicial, o horário AWS Backup receber um erro que permita que o trabalho seja repetido, AWS Backup tentará iniciá-lo automaticamente pelo menos a cada 10 minutos até que o backup seja iniciado com sucesso (o status do trabalho mude para`RUNNING`) ou até que o status do trabalho mude para `EXPIRED` (o que se espera que ocorra quando o tempo da janela inicial terminar).

Tipo: longo

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupRuleInput

Serviço: AWS Backup

Especifica uma tarefa programada usada para fazer backup de uma seleção de recursos.

Conteúdo

RuleName

Um nome de exibição para uma regra de backup. Deve conter de 1 a 50 caracteres alfanuméricos ou '-_.' .

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Exigido: Sim

TargetBackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Exigido: Sim

CompletionWindowMinutes

Um valor em minutos após um trabalho de backup ser iniciado com êxito antes que ele seja concluído ou ele será cancelado pelo AWS Backup. Este valor é opcional.

Tipo: longo

Obrigatório: não

CopyActions

Uma matriz de objetos `CopyAction`, que contém os detalhes da operação de cópia.

Tipo: matriz de objetos CopyAction

Obrigatório: não

EnableContinuousBackup

Especifica se AWS Backup cria backups contínuos. Causas verdadeiras AWS Backup para criar backups contínuos capazes de point-in-time restauração (PITR). Causas falsas (ou não especificadas) AWS Backup para criar backups instantâneos.

Tipo: booliano

Obrigatório: não

Lifecycle

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento refrigerado e quando ele expira. AWS Backup fará a transição e expirará os backups automaticamente de acordo com o ciclo de vida que você definir.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias a mais do que a configuração de “número de dias para a transição para o armazenamento frio”. A configuração “transição para frio após dias” não pode ser alterada após a transição de um backup para o armazenamento a frio.

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Esse parâmetro tem um valor máximo de 100 anos (36.500 dias).

Tipo: objeto Lifecycle

Obrigatório: Não

RecoveryPointTags

As tags a serem atribuídas aos recursos.

Tipo: mapa de string para string

Obrigatório: não

ScheduleExpression

Uma expressão CRON em UTC especificando quando AWS Backup inicia uma tarefa de backup.

Tipo: sequência

Obrigatório: não

ScheduleExpressionTimezone

O fuso horário no qual a expressão do cronograma está definida. Por padrão, ScheduleExpressions estão em UTC. É possível modificar isso para um fuso horário específico.

Tipo: sequência

Obrigatório: não

StartWindowMinutes

Um valor em minutos após a programação de um backup antes que um trabalho seja cancelado, se ele não for iniciado com êxito. Este valor é opcional. Se esse valor for incluído, deve ser de pelo menos 60 minutos para evitar erros.

Esse parâmetro tem um valor máximo de 100 anos (52.560.000 minutos).

Durante a janela inicial, o status do trabalho de backup permanece no status `CREATED` até que seja iniciado com êxito ou até que o tempo da janela inicial se esgote. Se, dentro da janela inicial, o horário AWS Backup receber um erro que permita que o trabalho seja repetido, AWS Backup tentará iniciá-lo automaticamente pelo menos a cada 10 minutos até que o backup seja iniciado com sucesso (o status do trabalho mude para`RUNNING`) ou até que o status do trabalho mude para `EXPIRED` (o que se espera que ocorra quando o tempo da janela inicial terminar).

Tipo: longo

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupSelection

Serviço: AWS Backup

Especifica um conjunto de recursos para um plano de backup.

Recomendamos que você especifique condições, tags ou recursos a serem incluídos ou excluídos. Caso contrário, o Backup tentará selecionar todos os recursos de armazenamento compatíveis e aceitos, o que pode ter implicações de custo não intencionais.

Para obter mais informações, consulte Atribuição programática de recursos.

Conteúdo

IamRoleArn

O ARN da função do IAM AWS Backup usada para autenticar ao fazer backup do recurso de destino; por exemplo,. `arn:aws:iam::123456789012:role/S3Access`

Tipo: string

Obrigatório: Sim

SelectionName

O nome de exibição de um documento de seleção de recursos. Deve conter de 1 a 50 caracteres alfanuméricos ou '-_.' .

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Exigido: Sim

Conditions

As condições que você define para atribuir recursos aos seus planos de backup usando tags. Por exemplo, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" }`.

`Conditions`suporta `StringEquals`,`StringLike`,`StringNotEquals`, `StringNotLike` e. Os operadores de condição diferenciam maiúsculas de minúsculas.

Se você especificar várias condições, os recursos corresponderão a todas as condições (e à lógica).

Tipo: objeto Conditions

Obrigatório: Não

ListOfTags

As condições que você define para atribuir recursos aos seus planos de backup usando tags. Por exemplo, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true"}`.

`ListOfTags`somente suporte`StringEquals`. Os operadores de condição diferenciam maiúsculas de minúsculas.

Se você especificar várias condições, os recursos corresponderão a qualquer uma das condições (lógica OR).

Tipo: matriz de objetos Condition

Obrigatório: não

NotResources

Os nomes de recursos da Amazon (ARNs) dos recursos a serem excluídos de um plano de backup. O número máximo de ARNs é 500 sem caracteres curinga ou 30 ARNs com curingas.

Se você precisar excluir muitos recursos de um plano de backup, considere uma estratégia de seleção de recursos diferente, como atribuir apenas um ou alguns tipos de recursos ou refinar sua seleção de recursos usando tags.

Tipo: matriz de strings

Obrigatório: não

Resources

Os nomes de recursos da Amazon (ARNs) dos recursos a serem atribuídos a um plano de backup. O número máximo de ARNs é 500 sem caracteres curinga ou 30 ARNs com curingas.

Se você precisar excluir muitos recursos de um plano de backup, considere uma estratégia de seleção de recursos diferente, como atribuir todos os recursos a um tipo de recursos ou refinar a seleção de recursos usando tags.

Se você especificar vários ARNs, os recursos corresponderão muito a qualquer um dos ARNs (lógica OR).

Tipo: matriz de strings

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupSelectionsListMember

Serviço: AWS Backup

Contém metadados sobre um objeto `BackupSelection`.

Conteúdo

BackupPlanId

Identifica exclusivamente um plano de backup.

Tipo: sequência

Obrigatório: não

CreationDate

A data e hora em que um plano de backup foi criada, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

CreatorRequestId

Uma string exclusiva que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Esse parâmetro é opcional.

Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

IamRoleArn

Especifica o nome do recurso da Amazon (ARN) do perfil do IAM para criar o ponto de recuperação de destino. Por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: sequência

Obrigatório: não

SelectionId

Identifica exclusivamente uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Tipo: sequência

Obrigatório: não

SelectionName

O nome de exibição de um documento de seleção de recursos.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupVaultListMember

Serviço: AWS Backup

Contém metadados sobre um cofre de backup.

Conteúdo

BackupVaultArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

Obrigatório: não

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Obrigatório: não

CreationDate

A data e a hora em que o plano de backup de um recurso foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

CreatorRequestId

Uma string exclusiva que identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Esse parâmetro é opcional.

Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

EncryptionKeyArn

Uma chave de criptografia do lado do servidor que você pode especificar para criptografar seus backups a partir de serviços que oferecem suporte ao AWS Backup gerenciamento completo; por exemplo,. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Se você especificar uma chave, deverá especificar seu ARN, e não seu alias. Se você não especificar uma chave, o AWS Backup criará uma chave do KMS para você por padrão.

Para saber quais AWS Backup serviços oferecem suporte ao AWS Backup gerenciamento completo e como AWS Backup lida com a criptografia para backups de serviços que ainda não oferecem suporte completo AWS Backup, consulte Criptografia para backups em AWS Backup

Tipo: sequência

Obrigatório: não

LockDate

A data e a hora em que a configuração do AWS Backup Vault Lock se torna imutável, o que significa que não pode ser alterada ou excluída.

Se tiver aplicado o Vault Lock ao seu cofre sem especificar uma data de bloqueio, você poderá alterar as configurações do Vault Lock ou excluir totalmente o Vault Lock do cofre a qualquer momento.

Esse valor está no formato Unix, Tempo Universal Coordenado (UTC) e tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

Locked

Um valor booleano que indica se o AWS Backup Vault Lock se aplica ao cofre de backup selecionado. Se `true`, o Vault Lock impede operações de exclusão e atualização nos pontos de recuperação no cofre selecionado.

Tipo: booliano

Obrigatório: não

MaxRetentionDays

A configuração do AWS Backup Vault Lock que especifica o período máximo de retenção em que o cofre retém seus pontos de recuperação. Se esse parâmetro não for especificado, o Vault Lock não aplicará um período máximo de retenção nos pontos de recuperação no cofre (permitindo o armazenamento indefinido).

Se esse parâmetro for especificado, qualquer trabalho de backup ou de cópia para o cofre deverá ter uma política de ciclo de vida com um período de retenção igual ou inferior ao período máximo de retenção. Se o período de retenção do trabalho for maior do que o período máximo de retenção, haverá falha no trabalho de backup ou de cópia do cofre e você deverá modificar as configurações do ciclo de vida ou usar um cofre diferente. Os pontos de recuperação já armazenados no cofre antes do Vault Lock não serão afetados.

Tipo: longo

Obrigatório: não

MinRetentionDays

A configuração do AWS Backup Vault Lock que especifica o período mínimo de retenção em que o cofre retém seus pontos de recuperação. Se esse parâmetro não for especificado, o Vault Lock não aplicará um período mínimo de retenção.

Se esse parâmetro for especificado, qualquer trabalho de backup ou de cópia para o cofre deverá ter uma política de ciclo de vida com um período de retenção igual ou superior ao período mínimo de retenção. Se o período de retenção do trabalho for inferior do que o período mínimo de retenção, haverá falha do cofre no trabalho de backup ou de cópia e você deverá modificar as configurações do ciclo de vida ou usar um cofre diferente. Os pontos de recuperação já armazenados no cofre antes do Vault Lock não serão afetados.

Tipo: longo

Obrigatório: não

NumberOfRecoveryPoints

O número de pontos de recuperação armazenados em um cofre de backup.

Tipo: longo

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CalculatedLifecycle

Serviço: AWS Backup

Contém os timestamps `DeleteAt` e `MoveToColdStorageAt`, que são usados para especificar o ciclo de vida de um ponto de recuperação.

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento refrigerado e quando ele expira. AWS Backup faz a transição e expira os backups automaticamente de acordo com o ciclo de vida definido por você.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias a mais do que a configuração de “número de dias para a transição para o armazenamento frio”. A configuração de "número de dias para transferência ao armazenamento 'frio'" não poderá ser alterada depois que um backup for transferido para o armazenamento "frio".

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Conteúdo

DeleteAt

Um timestamp que especifica quando excluir um ponto de recuperação.

Tipo: carimbo de data/hora

Obrigatório: não

MoveToColdStorageAt

Um timestamp que especifica quando fazer a transição de um ponto de recuperação para o armazenamento frio.

Tipo: carimbo de data/hora

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Condition

Serviço: AWS Backup

Contém uma matriz de tripletos composta por um tipo de condição (como `StringEquals`), uma chave e um valor. Usado para filtrar recursos usando suas tags e atribuí-los a um plano de backup. Diferencia maiúsculas e minúsculas.

Conteúdo

ConditionKey

A chave em um par de chave-valor. Por exemplo, na tag `Department: Accounting`, `Department` é a chave.

Tipo: string

Obrigatório: Sim

ConditionType

Uma operação aplicada a um par de chave/valor usado para atribuir recursos ao seu plano de backup. A condição só é compatível com `StringEquals`. Para opções de atribuição mais flexíveis, incluindo `StringLike` e a possibilidade de excluir recursos do seu plano de backup, use `Conditions` (com um “s” no final) para a `BackupSelection`.

Tipo: sequências

Valores Válidos: `STRINGEQUALS`

Obrigatório: Sim

ConditionValue

O valor em um par de chave-valor. Por exemplo, na tag `Department: Accounting`, `Accounting` é o valor.

Tipo: string

Obrigatório: Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ConditionParameter

Serviço: AWS Backup

Inclui informações sobre tags definidas para atribuir recursos marcados a um plano de backup.

Inclua o prefixo `aws:ResourceTag` em suas tags. Por exemplo, `"aws:ResourceTag/TagKey1": "Value1"`.

Conteúdo

ConditionKey

A chave em um par de chave-valor. Por exemplo, na tag `Department: Accounting`, `Department` é a chave.

Tipo: sequência

Obrigatório: não

ConditionValue

O valor em um par de chave-valor. Por exemplo, na tag `Department: Accounting`, `Accounting` é o valor.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Conditions

Serviço: AWS Backup

Contém informações sobre quais recursos incluir ou excluir de um plano de backup usando suas tags. As condições fazem distinção entre maiúsculas e minúsculas.

Conteúdo

StringEquals

Filtra os valores dos seus recursos marcados somente para os recursos que você marcou com o mesmo valor. Também chamada de "correspondência exata".

Tipo: matriz de objetos ConditionParameter

Obrigatório: não

StringLike

Filtra os valores dos recursos marcados para os valores de tag correspondentes com o uso de um caractere curinga (*) em qualquer posição na string. Por exemplo, "prod*" ou "*rod*" corresponde ao valor da tag “produção”.

Tipo: matriz de objetos ConditionParameter

Obrigatório: não

StringNotEquals

Filtra os valores dos recursos marcados somente para os recursos que você marcou que não têm o mesmo valor. Também chamada de "correspondência negada”.

Tipo: matriz de objetos ConditionParameter

Obrigatório: não

StringNotLike

Filtra os valores dos recursos marcados para valores de tag não correspondentes com o uso de um caractere curinga (*) em qualquer posição na string.

Tipo: matriz de objetos ConditionParameter

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ControlInputParameter

Serviço: AWS Backup

Os parâmetros de um controle. Um controle pode ter zero, um ou mais de um parâmetro. Um exemplo de controle com dois parâmetros é: “a frequência do plano de backup é pelo menos `daily` e o período de retenção é de pelo menos `1 year`“. O primeiro parâmetro é `daily`. O segundo parâmetro é `1 year`.

Conteúdo

ParameterName

O nome de um parâmetro, por exemplo, `BackupPlanFrequency`.

Tipo: sequência

Obrigatório: não

ParameterValue

O valor do parâmetro, por exemplo, `hourly`.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ControlScope

Serviço: AWS Backup

Uma framework consiste em um ou mais controles. Cada controle tem seu próprio escopo de controle. O escopo de controle pode incluir um ou mais tipos de recursos, uma combinação de chave e valor de tag, ou uma combinação de um tipo de recurso e um ID de recurso. Se nenhum escopo for especificado, as avaliações da regra serão acionadas quando qualquer recurso no grupo de registros for alterado na configuração.

> **Note**
>
> Para definir o escopo de um controle que inclua todo um recurso específico, deixe o `ControlScope` vazio ou não o passe ao chamar `CreateFramework`.

Conteúdo

ComplianceResourceIds

O ID do único AWS recurso que você deseja que seu escopo de controle contenha.

Tipo: Matriz de strings

Membros da Matriz: Número mínimo de 1 item. Número máximo de 100 itens.

Obrigatório: não

ComplianceResourceTypes

Descreve se o escopo do controle inclui um ou mais tipos de recursos, como `EFS` ou `RDS`.

Tipo: matriz de strings

Obrigatório: não

Tags

O par de chave-valor da tag aplicado aos AWS recursos que você deseja acionar uma avaliação para uma regra. No máximo um par chave-valor pode ser fornecido. O valor da tag é opcional, mas não pode ser uma string vazia se você estiver criando ou editando uma estrutura a partir do console (embora o valor possa ser uma string vazia quando incluído em um CloudFormation modelo).

A estrutura para atribuir uma tag é: `[{"Key":"string","Value":"string"}]`.

Tipo: mapa de string para string

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CopyAction

Serviço: AWS Backup

Os detalhes da operação de cópia.

Conteúdo

DestinationBackupVaultArn

Um nome de recurso da Amazon (ARN) que identifica exclusivamente o cofre de backup de destino para o backup copiado. Por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: string

Obrigatório: Sim

Lifecycle

Especifica o período, em dias, antes que um ponto de recuperação faça a transição para o armazenamento refrigerado ou seja excluído.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, no console, a configuração de retenção deve ser 90 dias maior do que a configuração de transição para frio após dias. A configuração de transição para frio após dias não pode ser alterada após a transição de um backup para frio.

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Para remover o ciclo de vida e os períodos de retenção existentes e manter seus pontos de recuperação indefinidamente, especifique -1 para e. `MoveToColdStorageAfterDays` `DeleteAfterDays`

Tipo: objeto Lifecycle

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CopyJob

Serviço: AWS Backup

Contém informações detalhadas sobre um trabalho de cópia.

Conteúdo

AccountId

O ID da conta proprietária do trabalho de cópia.

Tipo: string

Padrão: `^[0-9]{12}$`

Obrigatório: não

BackupSizeInBytes

O tamanho, em bytes, de um trabalho de cópia.

Tipo: longo

Obrigatório: não

ChildJobsInState

Isso retorna as estatísticas dos trabalhos de cópia filhos (aninhados) incluídos.

Tipo: mapa de string para string

Chaves válidas: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Obrigatório: não

CompletionDate

A data e hora em que um trabalho de cópia foi concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

CompositeMemberIdentifier

O identificador de um recurso em um grupo composto, como um ponto de recuperação aninhado (filho) pertencente a uma pilha composta (principal). O ID é transferido do ID lógico dentro de uma pilha.

Tipo: sequência

Obrigatório: não

CopyJobId

Identifica de forma exclusiva um trabalho de cópia.

Tipo: sequência

Obrigatório: não

CreatedBy

Contém informações sobre o plano de backup e a regra AWS Backup usados para iniciar o backup do ponto de recuperação.

Tipo: objeto RecoveryPointCreator

Obrigatório: Não

CreationDate

A data e hora em que um trabalho de cópia foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

DestinationBackupVaultArn

Um nome de recurso da Amazon (ARN) que identifica de forma exclusiva um cofre de backup. Por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

Obrigatório: não

DestinationRecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação de destino. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

Obrigatório: não

IamRoleArn

Especifica o ARN do perfil do IAM usado para copiar o ponto de recuperação de destino. Por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: sequência

Obrigatório: não

IsParent

Isso um valor booliano que indica que se trata de um trabalho de cópia pai (composto).

Tipo: booliano

Obrigatório: não

MessageCategory

Esse parâmetro é a contagem de trabalhos para a categoria de mensagem especificada.

Exemplos de strings podem incluir `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `InvalidParameters`. Consulte Monitoramento para obter uma lista de MessageCategory sequências de caracteres.

O valor ANY retorna a contagem de todas as categorias de mensagens.

`AGGREGATE_ALL` agrega as contagens de trabalhos de todas as categorias de mensagens e retorna a soma.

Tipo: sequência

Obrigatório: não

NumberOfChildJobs

O número de trabalhos de cópia secundários (aninhados).

Tipo: longo

Obrigatório: não

ParentJobId

Isso identifica de forma exclusiva uma solicitação para o AWS Backup copiar um recurso. O retorno será o ID do trabalho pai (composto).

Tipo: sequência

Obrigatório: não

ResourceArn

O AWS recurso a ser copiado; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Tipo: sequência

Obrigatório: não

ResourceName

O nome não exclusivo do recurso que pertence ao backup especificado.

Tipo: sequência

Obrigatório: não

ResourceType

O tipo de AWS recurso a ser copiado; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: não

SourceBackupVaultArn

Um nome de recurso da Amazon (ARN) que identifica de forma exclusiva um cofre de backup. Por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

Obrigatório: não

SourceRecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação de origem. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

Obrigatório: não

State

O estado atual de um trabalho de cópia.

Tipo: sequências

Valores Válidos: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Obrigatório: não

StatusMessage

Uma mensagem detalhada explicando o status do trabalho para copiar um recurso.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

CopyJobSummary

Serviço: AWS Backup

Isso é um resumo dos trabalhos de cópia criados ou em execução nos últimos 30 dias.

O resumo retornado pode conter o seguinte: Região, Conta, Estado, RestourceType, MessageCategory, StartTime EndTime, e Contagem de trabalhos incluídos.

Conteúdo

AccountId

O ID da conta à qual os trabalhos no resumo pertencem.

Tipo: string

Padrão: `^[0-9]{12}$`

Obrigatório: não

Count

O valor como um número de trabalhos em um resumo do trabalhos.

Tipo: inteiro

Obrigatório: não

EndTime

O valor do horário de término de um trabalho em formato numérico.

Esse valor é o horário no formato Unix, Tempo Universal Coordenado (UTC), e com precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

MessageCategory

Esse parâmetro é a contagem de trabalhos para a categoria de mensagem especificada.

Exemplos de strings incluem `AccessDenied`, `Success` e `InvalidParameters`. Consulte Monitoramento para obter uma lista de MessageCategory sequências de caracteres.

O valor ANY retorna a contagem de todas as categorias de mensagens.

AGGREGATE_ALL agrega as contagens de trabalhos de todas as categorias de mensagens e retorna a soma.

Tipo: sequência

Obrigatório: não

Region

As AWS regiões dentro do resumo do trabalho.

Tipo: sequência

Obrigatório: não

ResourceType

Esse valor é a contagem de trabalhos para o tipo de recurso especificado. A solicitação GetSupportedResourceTypes retorna strings para os tipos de recurso compatíveis.

Tipo: string

Padrão: ^[a-zA-Z0-9\-_\.]{1,50}$

Obrigatório: não

StartTime

O valor do horário de início de um trabalho em formato numérico.

Esse valor é o horário no formato Unix, Tempo Universal Coordenado (UTC), e com precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

State

Esse valor é a contagem dos trabalhos com o estado especificado.

Tipo: sequências

Valores Válidos: `CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DateRange

Serviço: AWS Backup

Este é um filtro de recursos contendo FromDate: DateTime e ToDate: DateTime. Ambos os valores são necessários. DateTime Valores futuros não são permitidos.

A data e a hora estão no formato Unix e no Tempo Universal Coordenado (UTC) e têm precisão de milissegundos (os milissegundos são opcionais). Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Conteúdo

FromDate

Esse valor é a data de início, inclusive.

A data e a hora estão no formato Unix e Tempo Universal Coordenado (UTC) e têm precisão de milissegundos (milissegundos são opcionais).

Tipo: carimbo de data/hora

Obrigatório: Sim

ToDate

Esse valor é a data de término, inclusive.

A data e a hora estão no formato Unix e Tempo Universal Coordenado (UTC) e têm precisão de milissegundos (milissegundos são opcionais).

Tipo: carimbo de data/hora

Obrigatório: Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Framework

Serviço: AWS Backup

Contém informações detalhadas sobre uma framework. As frameworks contêm controles que avaliam e relatam seus eventos e recursos de backup. As frameworks geram resultados diários de conformidade.

Conteúdo

CreationTime

A data e a hora em que a framework é criada, na representação ISO 8601. O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, 2020-07-10T15:00:00.000-08:00 representa o dia 10 de julho de 2020 às 15:00, 8 horas antes do UTC.

Tipo: carimbo de data/hora

Obrigatório: não

DeploymentStatus

O status de implantação de uma framework. Os status são:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Tipo: sequência

Obrigatório: não

FrameworkArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

Obrigatório: não

FrameworkDescription

Uma descrição opcional da framework com no máximo 1.024 caracteres.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 1.024.

Padrão: `.*\S.*`

Obrigatório: não

FrameworkName

O nome exclusivo de uma framework. Esse nome tem entre 1 e 256 caracteres, começando com uma letra, e consiste em letras (a-z, A-Z), números (0-9) e sublinhados (_).

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Obrigatório: não

NumberOfControls

O número de controles contidos na framework.

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

FrameworkControl

Serviço: AWS Backup

Contém informações detalhadas sobre todos os controles de um framework. Cada framework deve conter pelo menos um controle.

Conteúdo

ControlName

O nome de um controle. Esse nome tem entre 1 e 256 caracteres.

Tipo: string

Obrigatório: Sim

ControlInputParameters

Os pares de nome/valor.

Tipo: matriz de objetos ControlInputParameter

Obrigatório: não

ControlScope

O escopo de um controle. O escopo do controle define o que o controle avaliará. Três exemplos de escopos de controle são: um plano de backup específico, todos os planos de backup com uma tag específica ou todos os planos de backup.

Para obter mais informações, consulte `ControlScope.`

Tipo: objeto ControlScope

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

KeyValue

Serviço: AWS Backup

Par de duas strings relacionadas. Os caracteres permitidos são letras, espaços em branco e números que podem ser representados em UTF-8 e os seguintes caracteres: `+ - = . _ : /`.

Conteúdo

Key

A chave da tag (String). A chave não pode começar com `aws:`.

Restrições de Tamanho: Tamanho mínimo 1. O tamanho máximo é 128.

Padrão: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Tipo: string

Obrigatório: Sim

Value

O valor da chave.

Restrições de tamanho: o tamanho máximo é 256.

Padrão: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Tipo: string

Obrigatório: Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

LegalHold

Serviço: AWS Backup

Uma retenção legal é uma ferramenta administrativa que ajuda a evitar que os backups sejam excluídos enquanto estão em retenção. Enquanto a retenção estiver em vigor, não será possível excluir os backups em retenção, e as políticas de ciclo de vida que alterariam o status do backup (como a transição para armazenamento frio) serão adiadas até que a retenção legal seja removida. Um backup pode ter mais de uma retenção legal. As retenções legais são aplicadas a um ou mais backups (também conhecidos como pontos de recuperação). Esses backups podem ser filtrados por tipos de recursos e por IDs de recursos.

Conteúdo

CancellationDate

A hora em que a retenção legal foi cancelada.

Tipo: carimbo de data/hora

Obrigatório: não

CreationDate

A hora em que a retenção legal foi criada.

Tipo: carimbo de data/hora

Obrigatório: não

Description

A descrição de uma retenção legal.

Tipo: sequência

Obrigatório: não

LegalHoldArn

O nome de recurso da Amazon (ARN) da retenção legal; por exemplo,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipo: sequência

Obrigatório: não

LegalHoldId

O ID da retenção legal.

Tipo: sequência

Obrigatório: não

Status

O status da retenção legal.

Tipo: sequências

Valores Válidos: `CREATING | ACTIVE | CANCELING | CANCELED`

Obrigatório: não

Title

O título de uma retenção legal.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Lifecycle

Serviço: AWS Backup

Especifica o período de tempo, em dias, antes que um ponto de recuperação faça a transição para o armazenamento refrigerado ou seja excluído.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, no console, a configuração de retenção deve ser 90 dias maior do que a configuração de transição para frio após dias. A configuração de transição para frio após dias não pode ser alterada após a transição de um backup para frio.

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Para remover o ciclo de vida e os períodos de retenção existentes e manter seus pontos de recuperação indefinidamente, especifique -1 para e. `MoveToColdStorageAfterDays` `DeleteAfterDays`

Conteúdo

DeleteAfterDays

O número de dias após a criação em que um ponto de recuperação é excluído. Esse valor deve ser pelo menos 90 dias após o número de dias especificado em`MoveToColdStorageAfterDays`.

Tipo: longo

Obrigatório: não

MoveToColdStorageAfterDays

O número de dias após a criação em que um ponto de recuperação é movido para o armazenamento refrigerado.

Tipo: longo

Obrigatório: não

OptInToArchiveForSupportedResources

Se o valor for verdadeiro, seu plano de backup transferirá os recursos suportados para o nível de armazenamento (frio) de acordo com suas configurações de ciclo de vida.

Tipo: booliano

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ProtectedResource

Serviço: AWS Backup

Uma estrutura que contém informações sobre um recurso que teve backup feito.

Conteúdo

LastBackupTime

A data e hora em que o backup de um recurso foi feito pela última vez, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastBackupTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

LastBackupVaultArn

O ARN (Amazon Resource Name) do cofre de backup que contém o ponto de recuperação de backup mais recente.

Tipo: sequência

Obrigatório: não

LastRecoveryPointArn

O ARN (Amazon Resource Name) do ponto de recuperação mais recente.

Tipo: sequência

Obrigatório: não

ResourceArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

Obrigatório: não

ResourceName

O nome não exclusivo do recurso que pertence ao backup especificado.

Tipo: sequência

Obrigatório: não

ResourceType

O tipo de AWS recurso; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS). Para backups do Serviço de Cópias de Sombra de Volume (VSS) do Windows, o único tipo de recurso compatível é o Amazon EC2.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ProtectedResourceConditions

Serviço: AWS Backup

As condições que você define para os recursos em seu plano de teste de restauração usando tags.

Por exemplo, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Os operadores de condição diferenciam maiúsculas de minúsculas.

Conteúdo

StringEquals

Filtra os valores dos seus recursos marcados somente para os recursos que você marcou com o mesmo valor. Também chamada de "correspondência exata".

Tipo: matriz de objetos KeyValue

Obrigatório: não

StringNotEquals

Filtra os valores dos recursos marcados somente para os recursos que você marcou que não têm o mesmo valor. Também chamada de "correspondência negada”.

Tipo: matriz de objetos KeyValue

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointByBackupVault

Serviço: AWS Backup

Contém informações detalhadas sobre os pontos de recuperação armazenados em um cofre de backup.

Conteúdo

BackupSizeInBytes

O tamanho de um backup, em bytes.

Tipo: longo

Obrigatório: não

BackupVaultArn

Um ARN que identifica de forma exclusiva um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: sequência

Obrigatório: não

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Obrigatório: não

CalculatedLifecycle

Um objeto `CalculatedLifecycle` que contém os timestamps `DeleteAt` e `MoveToColdStorageAt`.

Tipo: objeto CalculatedLifecycle

Obrigatório: Não

CompletionDate

A data e hora em que um trabalho para restaurar um ponto de recuperação foi concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

CompositeMemberIdentifier

O identificador de um recurso em um grupo composto, como um ponto de recuperação aninhado (filho) pertencente a uma pilha composta (principal). O ID é transferido do ID lógico dentro de uma pilha.

Tipo: sequência

Obrigatório: não

CreatedBy

Contém informações de identificação sobre a criação de um ponto de recuperação, incluindo o `BackupPlanArn`, o `BackupPlanId`, a `BackupPlanVersion`, e o `BackupRuleId` do plano de backup usado para criá-lo.

Tipo: objeto RecoveryPointCreator

Obrigatório: Não

CreationDate

A data e hora em que um ponto de recuperação foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

EncryptionKeyArn

A chave de criptografia no lado do servidor usada para proteger seus backups, por exemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: sequência

Obrigatório: não

IamRoleArn

Especifica o ARN do perfil do IAM usado para criar o ponto de recuperação de destino. Por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: sequência

Obrigatório: não

IsEncrypted

Um valor booliano que é retornado como `TRUE` se o ponto de recuperação especificado estiver criptografado ou `FALSE` se o ponto de recuperação não estiver criptografado.

Tipo: booliano

Obrigatório: não

IsParent

Isso é um valor booliano que indica que se trata de um ponto de recuperação pai (composto).

Tipo: booliano

Obrigatório: não

LastRestoreTime

A data e hora em que um ponto de recuperação foi restaurado pela última vez, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastRestoreTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

Lifecycle

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento refrigerado e quando ele expira. AWS Backup faz a transição e expira os backups automaticamente de acordo com o ciclo de vida definido por você.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, a configuração de “retenção” deve ser 90 dias a mais do que a configuração de “número de dias para a transição para o armazenamento frio”. A configuração de "número de dias para transferência ao armazenamento 'frio'" não poderá ser alterada depois que um backup for transferido para o armazenamento "frio".

Os tipos de recursos que podem fazer a transição para o armazenamento refrigerado estão listados na tabela Disponibilidade de recursos por recursos. AWS Backup ignora essa expressão para outros tipos de recursos.

Tipo: objeto Lifecycle

Obrigatório: Não

ParentRecoveryPointArn

O Amazon Resource Name (ARN) do ponto de recuperação principal (composto).

Tipo: sequência

Obrigatório: não

RecoveryPointArn

Um Nome de recurso da Amazon (ARN) que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

Obrigatório: não

ResourceArn

Um ARN identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

Obrigatório: não

ResourceName

O nome não exclusivo do recurso que pertence ao backup especificado.

Tipo: sequência

Obrigatório: não

ResourceType

O tipo de AWS recurso salvo como ponto de recuperação; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS). Para backups do Serviço de Cópias de Sombra de Volume (VSS) do Windows, o único tipo de recurso compatível é o Amazon EC2.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: não

SourceBackupVaultArn

O cofre de backup do qual o ponto de recuperação foi copiado originalmente. Se o ponto de recuperação for restaurado na mesma conta, esse valor será `null`.

Tipo: sequência

Obrigatório: não

Status

Um código de status que especifica o estado do ponto de recuperação.

Tipo: sequências

Valores Válidos: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Obrigatório: não

StatusMessage

Uma mensagem explicando o status atual do ponto de recuperação.

Tipo: sequência

Obrigatório: não

VaultType

O tipo de cofre no qual o ponto de recuperação descrito é armazenado.

Tipo: sequências

Valores Válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointByResource

Serviço: AWS Backup

Contém informações detalhadas sobre um ponto de recuperação salvo.

Conteúdo

BackupSizeBytes

O tamanho de um backup, em bytes.

Tipo: longo

Obrigatório: não

BackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e a região da AWS em que são criados.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Obrigatório: não

CreationDate

A data e hora em que um ponto de recuperação foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

EncryptionKeyArn

A chave de criptografia no lado do servidor usada para proteger seus backups, por exemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: sequência

Obrigatório: não

IsParent

Isso é um valor booliano que indica que se trata de um ponto de recuperação pai (composto).

Tipo: booliano

Obrigatório: não

ParentRecoveryPointArn

O Amazon Resource Name (ARN) do ponto de recuperação principal (composto).

Tipo: sequência

Obrigatório: não

RecoveryPointArn

Um Nome de recurso da Amazon (ARN) que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

Obrigatório: não

ResourceName

O nome não exclusivo do recurso que pertence ao backup especificado.

Tipo: sequência

Obrigatório: não

Status

Um código de status que especifica o estado do ponto de recuperação.

Tipo: sequências

Valores Válidos: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Obrigatório: não

StatusMessage

Uma mensagem explicando o status atual do ponto de recuperação.

Tipo: sequência

Obrigatório: não

VaultType

O tipo de cofre no qual o ponto de recuperação descrito é armazenado.

Tipo: sequências

Valores Válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointCreator

Serviço: AWS Backup

Contém informações sobre o plano de backup e a regra AWS Backup usados para iniciar o backup do ponto de recuperação.

Conteúdo

BackupPlanArn

Um Nome do recurso da Amazon (ARN) que identifica exclusivamente um plano de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: sequência

Obrigatório: não

BackupPlanId

Identifica exclusivamente um plano de backup.

Tipo: sequência

Obrigatório: não

BackupPlanVersion

IDs de versão são strings Unicode exclusivas, geradas aleatoriamente, codificadas em UTF-8 com, no máximo, 1.024 bytes. Eles não podem ser editados.

Tipo: sequência

Obrigatório: não

BackupRuleId

Identifica de forma exclusiva uma regra usada para programar o backup de uma seleção de recursos.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointMember

Serviço: AWS Backup

Isso é um ponto de recuperação que é filho (aninhado) de um ponto de recuperação pai (composto). Esses pontos de recuperação podem ser desassociados do ponto de recuperação pai (composto). Nesse caso, eles não serão mais membros.

Conteúdo

BackupVaultName

O nome do cofre de backup (o contêiner lógico no qual os backups são armazenados).

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_]{2,50}$`

Obrigatório: não

RecoveryPointArn

O Amazon Resource Name (ARN) do ponto de recuperação principal (composto).

Tipo: sequência

Obrigatório: não

ResourceArn

O Amazon Resource Name (ARN) que identifica de forma exclusiva um recurso salvo.

Tipo: sequência

Obrigatório: não

ResourceType

O tipo de AWS recurso que é salvo como um ponto de recuperação.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointSelection

Serviço: AWS Backup

Isso especifica os critérios para atribuir um conjunto de recursos, como tipos de recursos ou cofres de backup.

Conteúdo

DateRange

Este é um filtro de recursos contendo FromDate: DateTime e ToDate: DateTime. Ambos os valores são necessários. DateTime Valores futuros não são permitidos.

A data e a hora estão no formato Unix e no Tempo Universal Coordenado (UTC) e têm precisão de milissegundos (os milissegundos são opcionais). Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: objeto DateRange

Obrigatório: Não

ResourceIdentifiers

Esses são os recursos incluídos na seleção de recursos (incluindo tipo de recursos e cofres).

Tipo: matriz de strings

Obrigatório: não

VaultNames

Esses são os nomes dos cofres que contêm os pontos de recuperação selecionados.

Tipo: matriz de strings

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

ReportDeliveryChannel

Serviço: AWS Backup

Contém informações do seu plano de relatório sobre onde entregar seus relatórios, especificamente o nome do bucket do Amazon S3, o prefixo de chave do S3 e os formatos dos relatórios.

Conteúdo

S3BucketName

O nome exclusivo do bucket do S3 que recebe os relatórios.

Tipo: string

Obrigatório: Sim

Formats

O formato dos seus relatórios:`CSV`,`JSON`, ou ambos. Se não especificado, o formato padrão será `CSV`.

Tipo: matriz de strings

Obrigatório: não

S3KeyPrefix

O prefixo de onde o AWS Backup Audit Manager entrega seus relatórios para o Amazon S3. O prefixo é essa parte do seguinte caminho: s3:///your-bucket-name/backup/us-west-2/year/month/day/report-name. `prefix` Se não for especificado, não haverá prefixo.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

ReportDestination

Serviço: AWS Backup

Contém informações do trabalho do relatório sobre o destino do relatório.

Conteúdo

S3BucketName

O nome exclusivo do bucket do Amazon S3 que recebe os relatórios.

Tipo: sequência

Obrigatório: não

S3Keys

O nome da chave do objeto que identifica de forma exclusiva os relatórios no bucket do S3.

Tipo: matriz de strings

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ReportJob

Serviço: AWS Backup

Contém informações detalhadas sobre um trabalho de relatório. Um trabalho de relatório compila um relatório com base em um plano de relatório e o publica no Amazon S3.

Conteúdo

CompletionTime

A data e hora em que um trabalho de relatório foi concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

CreationTime

A data e hora em que um trabalho de relatório foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

ReportDestination

O nome do bucket do S3 e as chaves do S3 para o destino em que o trabalho de relatório publica o relatório.

Tipo: objeto ReportDestination

Obrigatório: Não

ReportJobId

O identificador de um trabalho de relatório. Uma string Unicode exclusiva, gerada aleatoriamente, codificada em UTF-8, com, no máximo, 1.024 bytes. Não é possível editar os IDs de trabalho de relatório.

Tipo: sequência

Obrigatório: não

ReportPlanArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

Obrigatório: não

ReportTemplate

Identifica o modelo do relatório. Relatórios são criados utilizando um modelo de relatório. Os modelos de relatório são:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Tipo: sequência

Obrigatório: não

Status

O status de um trabalho de relatório. Os status são:

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED` significa que o relatório está disponível para análise no destino designado. Se o status for `FAILED`, analise a `StatusMessage` para ver o motivo.

Tipo: sequência

Obrigatório: não

StatusMessage

Uma mensagem explicando o status do trabalho de relatório.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ReportPlan

Serviço: AWS Backup

Contém informações detalhadas sobre um trabalho de relatório.

Conteúdo

CreationTime

A data e hora em que um plano de relatório foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

DeploymentStatus

O status de implantação de um plano de relatório. Os status são:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED`

Tipo: sequência

Obrigatório: não

LastAttemptedExecutionTime

A data e a hora da última tentativa de execução de um trabalho de relatório associado a esse plano de relatório, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastAttemptedExecutionTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

LastSuccessfulExecutionTime

A data e a hora da última tentativa de execução de um trabalho de relatório associado a esse plano de relatório, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastSuccessfulExecutionTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

ReportDeliveryChannel

Contém informações sobre onde e como entregar seus relatórios, especificamente o nome do bucket do Amazon S3, o prefixo de chave do S3 e os formatos dos relatórios.

Tipo: objeto ReportDeliveryChannel

Obrigatório: Não

ReportPlanArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

Obrigatório: não

ReportPlanDescription

Uma descrição opcional do plano de relatório com no máximo 1.024 caracteres.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 1.024.

Padrão: `.*\S.*`

Obrigatório: não

ReportPlanName

O nome exclusivo do plano de relatório. Esse nome tem entre 1 e 256 caracteres, começando com uma letra, e consiste em letras (a-z, A-Z), números (0-9) e sublinhados (_).

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. Comprimento máximo de 256.

Padrão: `[a-zA-Z][_a-zA-Z0-9]*`

Obrigatório: não

ReportSetting

Identifica o modelo do relatório. Relatórios são criados utilizando um modelo de relatório. Os modelos de relatório são:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Se o modelo de relatório for `RESOURCE_COMPLIANCE_REPORT` ou`CONTROL_COMPLIANCE_REPORT`, esse recurso de API também descreve a cobertura do relatório por Regiões da AWS estruturas.

Tipo: objeto ReportSetting

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ReportSetting

Serviço: AWS Backup

Contém informações detalhadas sobre uma configuração de relatório.

Conteúdo

ReportTemplate

Identifica o modelo do relatório. Relatórios são criados utilizando um modelo de relatório. Os modelos de relatório são:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Tipo: string

Obrigatório: Sim

Accounts

Essas são as contas a serem incluídas no relatório.

Use o valor da sequência de caracteres de `ROOT` para incluir todas as unidades organizacionais.

Tipo: matriz de strings

Obrigatório: não

FrameworkArns

Os nomes dos recursos da Amazon (ARNs) das estruturas cobertas por um relatório.

Tipo: matriz de strings

Obrigatório: não

NumberOfFrameworks

O número de frameworks que um relatório abrange.

Tipo: inteiro

Obrigatório: não

OrganizationUnits

Estas são as unidades organizacionais a serem incluídas no relatório.

Tipo: matriz de strings

Obrigatório: não

Regions

Essas são as regiões a serem incluídas no relatório.

Use o caractere curinga como valor da string para incluir todas as regiões.

Tipo: matriz de strings

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreJobCreator

Serviço: AWS Backup

Contém informações sobre o plano de testes de restauração que o AWS Backup utilizou para iniciar o trabalho de restauração.

Conteúdo

RestoreTestingPlanArn

Um nome do recurso da Amazon (ARN) que identifica exclusivamente um plano de testes de restauração.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreJobsListMember

Serviço: AWS Backup

Contém metadados sobre um trabalho de restauração.

Conteúdo

AccountId

O ID da conta proprietária do trabalho de restauração.

Tipo: string

Padrão: `^[0-9]{12}$`

Obrigatório: não

BackupSizeInBytes

O tamanho, em bytes, do recurso restaurado.

Tipo: longo

Obrigatório: não

CompletionDate

A data e hora em que um trabalho para restaurar um ponto de recuperação foi concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

CreatedBy

Contém informações de identificação sobre a criação de um trabalho de restauração.

Tipo: objeto RestoreJobCreator

Obrigatório: Não

CreatedResourceArn

Um Nome do recurso da Amazon (ARN) que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Tipo: sequência

Obrigatório: não

CreationDate

A data e hora em que um trabalho de restauração foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

DeletionStatus

Isso registra o status dos dados gerados pelo teste de restauração. O status pode ser `Deleting`, `Failed` ou `Successful`.

Tipo: sequências

Valores Válidos: `DELETING | FAILED | SUCCESSFUL`

Obrigatório: não

DeletionStatusMessage

Isso descreve o status de exclusão do trabalho de restauração.

Tipo: sequência

Obrigatório: não

ExpectedCompletionTimeMinutes

A quantidade de tempo, em minutos, que se espera que um trabalho de restauração de um ponto de recuperação leve.

Tipo: longo

Obrigatório: não

IamRoleArn

Especifica o ARN do perfil do IAM usado para criar o ponto de recuperação de destino. Por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: sequência

Obrigatório: não

PercentDone

Contém uma porcentagem estimada de conclusão de um trabalho no momento em que o status do trabalho foi consultado.

Tipo: sequência

Obrigatório: não

RecoveryPointArn

Um ARN que identifica de forma exclusiva um ponto de recuperação. Por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: sequência

Obrigatório: não

RecoveryPointCreationDate

A data em que um ponto de recuperação foi criado.

Tipo: carimbo de data/hora

Obrigatório: não

ResourceType

O tipo de recurso dos trabalhos de restauração listados. Por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS). Para backups do Serviço de Cópias de Sombra de Volume (VSS) do Windows, o único tipo de recurso compatível é o Amazon EC2.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: não

RestoreJobId

Identifica de forma exclusiva a tarefa que restaura um ponto de recuperação.

Tipo: sequência

Obrigatório: não

Status

Um código de status que especifica o estado do trabalho iniciado AWS Backup para restaurar um ponto de recuperação.

Tipo: sequências

Valores Válidos: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

Obrigatório: não

StatusMessage

Uma mensagem detalhada explicando o status do trabalho para restaurar um ponto de recuperação.

Tipo: sequência

Obrigatório: não

ValidationStatus

O status da validação executada na tarefa de restauração indicada.

Tipo: sequências

Valores Válidos: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Obrigatório: não

ValidationStatusMessage

Isso descreve o status da validação executada no trabalho de restauração indicado.

Tipo: sequência

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreJobSummary

Serviço: AWS Backup

Isso é um resumo dos trabalhos de restauração criados ou em execução nos últimos 30 dias.

O resumo retornado pode conter o seguinte: Região, Conta, Estado, ResourceType, MessageCategory, StartTime EndTime, e Contagem de trabalhos incluídos.

Conteúdo

AccountId

O ID da conta à qual os trabalhos no resumo pertencem.

Tipo: string

Padrão: `^[0-9]{12}$`

Obrigatório: não

Count

O valor como um número de trabalhos em um resumo do trabalhos.

Tipo: inteiro

Obrigatório: não

EndTime

O valor do horário de término de um trabalho em formato numérico.

Esse valor é o horário no formato Unix, Tempo Universal Coordenado (UTC), e com precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

Region

As AWS regiões no resumo do trabalho.

Tipo: sequência

Obrigatório: não

ResourceType

Esse valor é a contagem de trabalhos para o tipo de recurso especificado. A solicitação `GetSupportedResourceTypes` retorna strings para os tipos de recurso compatíveis.

Tipo: string

Padrão: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obrigatório: não

StartTime

O valor do horário de início de um trabalho em formato numérico.

Esse valor é o horário no formato Unix, Tempo Universal Coordenado (UTC), e com precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

State

Esse valor é a contagem dos trabalhos com o estado especificado.

Tipo: sequências

Valores Válidos: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

RestoreTestingPlanForCreate

Serviço: AWS Backup

Contém metadados sobre um plano de testes de restauração.

Conteúdo

RecoveryPointSelection

`RecoveryPointSelection`tem cinco parâmetros (três obrigatórios e dois opcionais). Os valores que você especifica determinam qual ponto de recuperação está incluído no teste de restauração. Você deve indicar com `Algorithm` se deseja o ponto de recuperação mais recente dentro do seu `SelectionWindowDays` ou se deseja um ponto de recuperação aleatório e deve indicar por meio `IncludeVaults` de quais cofres os pontos de recuperação podem ser escolhidos.

`Algorithm`(obrigatório) Valores válidos: "`LATEST_WITHIN_WINDOW`" ou "`RANDOM_WITHIN_WINDOW`".

`Recovery point types`(obrigatório) Valores válidos: "`SNAPSHOT`" e/ou "`CONTINUOUS`". `SNAPSHOT`Inclua para restaurar somente pontos de recuperação de instantâneos; `CONTINUOUS` inclua para restaurar pontos de recuperação contínuos (restauração pontual /PITR); use ambos para restaurar um instantâneo ou um ponto de recuperação contínuo. O ponto de recuperação será determinado pelo valor de`Algorithm`.

`IncludeVaults`(obrigatório). Você deve incluir um ou mais cofres de backup. Use o caractere curinga ["`*`"] ou ARNs específicos.

`SelectionWindowDays`(opcional) O valor deve ser um número inteiro (em dias) de 1 a 365. Se não for incluído, o valor padrão será. `30`

`ExcludeVaults`(opcional). Você pode optar por inserir um ou mais ARNs específicos do cofre de backup para excluir o conteúdo desses cofres da elegibilidade para restauração. Ou você pode incluir uma lista de seletores. Se esse parâmetro e seu valor não forem incluídos, o padrão será uma lista vazia.

Tipo: objeto RestoreTestingRecoveryPointSelection

Obrigatório: Sim

RestoreTestingPlanName

RestoreTestingPlanName É uma string exclusiva que é o nome do plano de teste de restauração. Ele não pode ser alterado após a criação e deve consistir somente em caracteres alfanuméricos e sublinhados.

Tipo: string

Obrigatório: Sim

ScheduleExpression

Uma expressão cron no fuso horário especificado quando um plano de testes de restauração é executado.

Tipo: string

Obrigatório: Sim

ScheduleExpressionTimezone

Opcional. O fuso horário no qual a expressão de programação foi definida. Por padrão, ScheduleExpressions estão em UTC. É possível modificar isso para um fuso horário específico.

Tipo: sequência

Obrigatório: não

StartWindowHours

O padrão é 24 horas.

Quantidade de horas que um teste de restauração tem para ser iniciado após sua programação, antes que o trabalho seja cancelado. Este valor é opcional. Se esse valor for incluído, o parâmetro terá um valor máximo de 168 horas (uma semana).

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingPlanForGet

Serviço: AWS Backup

Contém metadados sobre um plano de testes de restauração.

Conteúdo

CreationTime

A data e hora em que um plano de testes de restauração foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: Sim

RecoveryPointSelection

Os critérios especificados para atribuir um conjunto de recursos, como tipos de ponto de recuperação ou cofres de backup.

Tipo: objeto RestoreTestingRecoveryPointSelection

Obrigatório: Sim

RestoreTestingPlanArn

Um nome do recurso da Amazon (ARN) que identifica exclusivamente um plano de testes de restauração.

Tipo: string

Obrigatório: Sim

RestoreTestingPlanName

O nome do plano de teste de restauração.

Tipo: string

Obrigatório: Sim

ScheduleExpression

Uma expressão cron no fuso horário especificado quando um plano de testes de restauração é executado.

Tipo: string

Obrigatório: Sim

CreatorRequestId

Identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Se a solicitação incluir um `CreatorRequestId` que corresponda a um plano de backup existente, esse plano será retornado. Esse parâmetro é opcional.

Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

LastExecutionTime

A última vez que um teste de restauração foi executado com o plano de testes de restauração especificado. A data e a hora devem estar em formato Unix e UTC (Tempo Universal Coordenado). O valor de `LastExecutionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

LastUpdateTime

A data e hora em que o plano de testes de restauração foi atualizado. Essa atualização está em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastUpdateTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

ScheduleExpressionTimezone

Opcional. O fuso horário no qual a expressão de programação foi definida. Por padrão, ScheduleExpressions estão em UTC. É possível modificar isso para um fuso horário específico.

Tipo: sequência

Obrigatório: não

StartWindowHours

O padrão é 24 horas.

Quantidade de horas que um teste de restauração tem para ser iniciado após sua programação, antes que o trabalho seja cancelado. Este valor é opcional. Se esse valor for incluído, o parâmetro terá um valor máximo de 168 horas (uma semana).

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingPlanForList

Serviço: AWS Backup

Contém metadados sobre um plano de testes de restauração.

Conteúdo

CreationTime

A data e hora em que um plano de testes de restauração foi criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: Sim

RestoreTestingPlanArn

Um nome do recurso da Amazon (ARN) que identifica exclusivamente um plano de testes de restauração.

Tipo: string

Obrigatório: Sim

RestoreTestingPlanName

O nome do plano de teste de restauração.

Tipo: string

Obrigatório: Sim

ScheduleExpression

Uma expressão cron no fuso horário especificado quando um plano de testes de restauração é executado.

Tipo: string

Obrigatório: Sim

LastExecutionTime

A última vez que um teste de restauração foi executado com o plano de testes de restauração especificado. A data e a hora devem estar em formato Unix e UTC (Tempo Universal

Coordenado). O valor de `LastExecutionDate` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

LastUpdateTime

A data e hora em que o plano de testes de restauração foi atualizado. Essa atualização está em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastUpdateTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: não

ScheduleExpressionTimezone

Opcional. O fuso horário no qual a expressão de programação foi definida. Por padrão, ScheduleExpressions estão em UTC. É possível modificar isso para um fuso horário específico.

Tipo: sequência

Obrigatório: não

StartWindowHours

O padrão é 24 horas.

Quantidade de horas que um teste de restauração tem para ser iniciado após sua programação, antes que o trabalho seja cancelado. Este valor é opcional. Se esse valor for incluído, o parâmetro terá um valor máximo de 168 horas (uma semana).

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingPlanForUpdate

Serviço: AWS Backup

Contém metadados sobre um plano de testes de restauração.

Conteúdo

RecoveryPointSelection

Obrigatório: `Algorithm`; `RecoveryPointTypes`; `IncludeVaults` (um ou mais).

Opcional: SelectionWindowDays('30' se não for especificado); `ExcludeVaults` (o padrão é uma lista vazia se não estiver listada).

Tipo: objeto RestoreTestingRecoveryPointSelection

Obrigatório: Não

ScheduleExpression

Uma expressão cron no fuso horário especificado quando um plano de testes de restauração é executado.

Tipo: sequência

Obrigatório: não

ScheduleExpressionTimezone

Opcional. O fuso horário no qual a expressão de programação foi definida. Por padrão, ScheduleExpressions estão em UTC. É possível modificar isso para um fuso horário específico.

Tipo: sequência

Obrigatório: não

StartWindowHours

O padrão é 24 horas.

Quantidade de horas que um teste de restauração tem para ser iniciado após sua programação, antes que o trabalho seja cancelado. Este valor é opcional. Se esse valor for incluído, o parâmetro terá um valor máximo de 168 horas (uma semana).

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingRecoveryPointSelection

Serviço: AWS Backup

`RecoveryPointSelection`tem cinco parâmetros (três obrigatórios e dois opcionais). Os valores que você especifica determinam qual ponto de recuperação está incluído no teste de restauração. Você deve indicar com `Algorithm` se deseja o ponto de recuperação mais recente dentro do seu `SelectionWindowDays` ou se deseja um ponto de recuperação aleatório e deve indicar por meio `IncludeVaults` de quais cofres os pontos de recuperação podem ser escolhidos.

`Algorithm`(obrigatório) Valores válidos: "`LATEST_WITHIN_WINDOW`" ou "`RANDOM_WITHIN_WINDOW`".

`Recovery point types`(obrigatório) Valores válidos: "`SNAPSHOT`" e/ou "`CONTINUOUS`". `SNAPSHOT`Inclua para restaurar somente pontos de recuperação de instantâneos; `CONTINUOUS` inclua para restaurar pontos de recuperação contínuos (restauração pontual /PITR); use ambos para restaurar um instantâneo ou um ponto de recuperação contínuo. O ponto de recuperação será determinado pelo valor de`Algorithm`.

`IncludeVaults`(obrigatório). Você deve incluir um ou mais cofres de backup. Use o caractere curinga ["*"] ou ARNs específicos.

`SelectionWindowDays`(opcional) O valor deve ser um número inteiro (em dias) de 1 a 365. Se não for incluído, o valor padrão será. `30`

`ExcludeVaults`(opcional). Você pode optar por inserir um ou mais ARNs específicos do cofre de backup para excluir o conteúdo desses cofres da elegibilidade para restauração. Ou você pode incluir uma lista de seletores. Se esse parâmetro e seu valor não forem incluídos, o padrão será uma lista vazia.

Conteúdo

Algorithm

Os valores aceitáveis incluem “LATEST_WITHIN_WINDOW” ou “RANDOM_WITHIN_WINDOW”.

Tipo: sequências

Valores Válidos: `LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW`

Obrigatório: não

ExcludeVaults

Os valores aceitos incluem ARNs específicos ou uma lista de seletores. O padrão será uma lista vazia se não estiver listado.

Tipo: matriz de strings

Obrigatório: não

IncludeVaults

Os valores aceitos incluem o caractere curinga [“*”], ARNs específicos ou substituição de caractere curinga de ARN [“arn:aws:backup:us-west-2:123456789012:backup-vault:asdf”, ...] [“arn:aws:backup:*:*:backup-vault:asdf-*”, ...]

Tipo: matriz de strings

Obrigatório: não

RecoveryPointTypes

Esses são os tipos de ponto de recuperação.

SNAPSHOTInclua para restaurar somente pontos de recuperação de instantâneos; CONTINUOUS inclua para restaurar pontos de recuperação contínuos (restauração pontual /PITR); use ambos para restaurar um instantâneo ou um ponto de recuperação contínuo. O ponto de recuperação será determinado pelo valor de`Algorithm`.

Tipo: matriz de strings

Valores Válidos: `CONTINUOUS | SNAPSHOT`

Obrigatório: não

SelectionWindowDays

Os valores aceitos são números inteiros de 1 a 365.

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingSelectionForCreate

Serviço: AWS Backup

Contém metadados sobre uma seleção de testes de restauração específica.

ProtectedResourceType é obrigatório, como Amazon EBS ou Amazon EC2.

Isso consiste em `RestoreTestingSelectionName`, `ProtectedResourceType` e um dos seguintes:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Cada tipo de recurso protegido pode ter um único valor.

Uma seleção de testes de restauração pode incluir um valor curinga (“*”) para `ProtectedResourceArns` com `ProtectedResourceConditions`. Como alternativa, você pode incluir até 30 ARNs de recursos protegidos específicos em `ProtectedResourceArns`.

Exemplos de `ProtectedResourceConditions` incluem `StringEquals` e `StringNotEquals`.

Conteúdo

IamRoleArn

O nome do recurso da Amazon (ARN) do perfil do IAM que o AWS Backup usa para criar o recurso de destino. Por exemplo: `arn:aws:iam::123456789012:role/S3Access`.

Tipo: string

Obrigatório: Sim

ProtectedResourceType

O tipo de AWS recurso incluído em uma seleção de teste de restauração; por exemplo, um volume do Amazon EBS ou um banco de dados do Amazon RDS.

Os tipos de recurso compatíveis e aceitos incluem:

- `Aurora` para Amazon Aurora
- `DocumentDB` para Amazon DocumentDB (compatível com MongoDB)

- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store
- `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: string

Obrigatório: Sim

RestoreTestingSelectionName

O nome exclusivo da seleção de teste de restauração que pertence ao plano de teste de restauração relacionado.

Tipo: string

Obrigatório: Sim

ProtectedResourceArns

Cada recurso protegido pode ser filtrado por seus ARNs específicos, como `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`, ou por um caractere curinga (`ProtectedResourceArns: ["*"]`), mas não por ambos.

Tipo: matriz de strings

Obrigatório: não

ProtectedResourceConditions

Se você incluiu o caractere curinga ProtectedResourceArns, pode incluir condições de recursos, como`ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }]`.

Tipo: objeto ProtectedResourceConditions

Obrigatório: Não

RestoreMetadataOverrides

Você pode substituir determinadas chaves de metadados de restauração incluindo o parâmetro `RestoreMetadataOverrides` no corpo de `RestoreTestingSelection`. Os valores de chave não diferenciam entrem maiúsculas e minúsculas.

Veja a lista completa de Metadados inferidos de testes de restauração.

Tipo: mapa de string para string

Obrigatório: não

ValidationWindowHours

Essa é a quantidade de horas (de 1 a 168) disponíveis para executar um script de validação nos dados. Os dados serão excluídos após a conclusão do script de validação ou no final do período de retenção especificado, o que ocorrer primeiro.

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingSelectionForGet

Serviço: AWS Backup

Contém metadados sobre uma seleção de testes de restauração.

Conteúdo

CreationTime

A data e hora em que uma seleção de testes de restauração foi criada, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: Sim

IamRoleArn

O nome do recurso da Amazon (ARN) do perfil do IAM que o AWS Backup usa para criar o recurso de destino. Por exemplo: `arn:aws:iam::123456789012:role/S3Access`.

Tipo: string

Obrigatório: Sim

ProtectedResourceType

O tipo de AWS recurso incluído em uma seleção de teste de recursos; por exemplo, um volume do Amazon EBS ou um banco de dados do Amazon RDS.

Tipo: string

Obrigatório: Sim

RestoreTestingPlanName

RestoreTestingPlanName É uma string exclusiva que é o nome do plano de teste de restauração.

Tipo: string

Obrigatório: Sim

RestoreTestingSelectionName

O nome exclusivo da seleção de teste de restauração que pertence ao plano de teste de restauração relacionado.

Tipo: string

Obrigatório: Sim

CreatorRequestId

Identifica a solicitação e permite que as solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes. Se a solicitação incluir um `CreatorRequestId` que corresponda a um plano de backup existente, esse plano será retornado. Esse parâmetro é opcional.

Se usado, esse parâmetro deve conter de 1 a 50 caracteres alfanuméricos ou “-_” .

Tipo: sequência

Obrigatório: não

ProtectedResourceArns

Você pode incluir ARNs específicos, como `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`, ou pode incluir um caractere curinga (`ProtectedResourceArns: ["*"]`), mas não ambos.

Tipo: matriz de strings

Obrigatório: não

ProtectedResourceConditions

Em uma seleção de testes de recursos, esse parâmetro é filtrado por condições específicas, como `StringEquals` ou `StringNotEquals`.

Tipo: objeto ProtectedResourceConditions

Obrigatório: Não

RestoreMetadataOverrides

Você pode substituir determinadas chaves de metadados de restauração incluindo o parâmetro `RestoreMetadataOverrides` no corpo de `RestoreTestingSelection`. Os valores de chave não diferenciam entrem maiúsculas e minúsculas.

Veja a lista completa de Metadados inferidos de testes de restauração.

Tipo: mapa de string para string

Obrigatório: não

ValidationWindowHours

Essa é a quantidade de horas (de 1 a 168) disponíveis para executar um script de validação nos dados. Os dados serão excluídos após a conclusão do script de validação ou no final do período de retenção especificado, o que ocorrer primeiro.

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingSelectionForList

Serviço: AWS Backup

Contém metadados sobre uma seleção de testes de restauração.

Conteúdo

CreationTime

A data e hora em que uma seleção de testes de restauração foi criada, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationTime` tem precisão de milissegundos. Por exemplo, o valor 1516925490,087 representa sexta-feira, 26 de janeiro de 2018, 0:11:30,087.

Tipo: carimbo de data/hora

Obrigatório: Sim

IamRoleArn

O nome do recurso da Amazon (ARN) do perfil do IAM que o AWS Backup usa para criar o recurso de destino. Por exemplo: `arn:aws:iam::123456789012:role/S3Access`.

Tipo: string

Obrigatório: Sim

ProtectedResourceType

O tipo de AWS recurso incluído em uma seleção de teste de restauração; por exemplo, um volume do Amazon EBS ou um banco de dados do Amazon RDS.

Tipo: string

Obrigatório: Sim

RestoreTestingPlanName

Essa string exclusiva é o nome do plano de testes de restauração.

O nome não poderá ser alterado após a criação. Ele só pode conter caracteres alfanuméricos e sublinhados. O tamanho máximo é 50.

Tipo: string

Obrigatório: Sim

RestoreTestingSelectionName

Nome exclusivo de uma seleção de testes de restauração.

Tipo: string

Obrigatório: Sim

ValidationWindowHours

Esse valor representa o tempo, em horas, em que os dados são retidos após um teste de restauração para que a validação opcional possa ser concluída.

O valor aceito é um número inteiro entre 0 e 168 (o equivalente a sete dias).

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingSelectionForUpdate

Serviço: AWS Backup

Contém metadados sobre uma seleção de testes de restauração.

Conteúdo

IamRoleArn

O nome do recurso da Amazon (ARN) do perfil do IAM que o AWS Backup usa para criar o recurso de destino. Por exemplo: `arn:aws:iam::123456789012:role/S3Access`.

Tipo: sequência

Obrigatório: não

ProtectedResourceArns

Você pode incluir uma lista de ARNs específicos, como `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`, ou pode incluir um caractere curinga (`ProtectedResourceArns: ["*"]`), mas não ambos.

Tipo: matriz de strings

Obrigatório: não

ProtectedResourceConditions

As condições que você define para os recursos em seu plano de teste de restauração usando tags.

Por exemplo, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Os operadores de condição diferenciam maiúsculas de minúsculas.

Tipo: objeto ProtectedResourceConditions

Obrigatório: Não

RestoreMetadataOverrides

Você pode substituir determinadas chaves de metadados de restauração incluindo o parâmetro `RestoreMetadataOverrides` no corpo de `RestoreTestingSelection`. Os valores de chave não diferenciam entrem maiúsculas e minúsculas.

Veja a lista completa de Metadados inferidos de testes de restauração.

Tipo: mapa de string para string

Obrigatório: não

ValidationWindowHours

Esse valor representa o tempo, em horas, em que os dados são retidos após um teste de restauração para que a validação opcional possa ser concluída.

O valor aceito é um número inteiro entre 0 e 168 (o equivalente a sete dias).

Tipo: inteiro

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

AWS Backup gateway

Os seguintes tipos de dados são compatíveis com o AWS Backup gateway:

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine

- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

Serviço: AWS Backup gateway

Descreve um intervalo limite de taxa de largura de banda para um gateway. Uma programação de limite de taxa de largura de banda consiste em um ou mais intervalos de limite de taxa de largura de banda. Um intervalo de limite de taxa de largura de banda define um período em um ou mais dias da semana, durante o qual os limites de taxa de largura de banda são especificados para upload, download ou ambos.

Conteúdo

DaysOfWeek

O componente de dias da semana do intervalo limite da taxa de largura de banda, representado como números ordinais de 0 a 6, em que 0 representa domingo e 6 representa sábado.

Tipo: matriz de números inteiros

Membros da Matriz: Número mínimo de 1 item. Número máximo de 7 itens.

Intervalo válido: valor mínimo de 0. Valor máximo de 6.

Obrigatório: Sim

EndHourOfDay

A hora do dia para encerrar o intervalo do limite da taxa de largura de banda.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 23.

Obrigatório: Sim

EndMinuteOfHour

O minuto da hora para encerrar o intervalo do limite da taxa de largura de banda.

> **Important**
>
> O intervalo do limite da taxa de largura de banda termina no final do minuto. Para encerrar um intervalo ao final de uma hora, use o valor 59.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 59.

Obrigatório: Sim

StartHourOfDay

A hora do dia para iniciar o intervalo do limite da taxa de largura de banda.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 23.

Obrigatório: Sim

StartMinuteOfHour

O minuto da hora para iniciar o intervalo do limite da taxa de largura de banda. O intervalo inicia no início desse minuto. Para iniciar um intervalo exatamente no início da hora, use o valor `0`.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 59.

Obrigatório: Sim

AverageUploadRateLimitInBitsPerSec

O componente do limite médio da taxa de upload do intervalo limite da taxa de largura de banda, em bits por segundo. Esse campo não será exibido na resposta se o limite da taxa de upload não estiver definido.

Tipo: longo

Intervalo válido: valor mínimo de 51.200. Valor máximo de 8.000.000.000.000.

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

Gateway

Serviço: AWS Backup gateway

Um gateway é um dispositivo AWS Backup Gateway executado na rede do cliente para fornecer conectividade perfeita ao armazenamento de backup na AWS nuvem.

Conteúdo

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway. Use a `ListGateways` operação para retornar uma lista de gateways para sua conta e. Região da AWS

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obrigatório: não

GatewayDisplayName

O nome de exibição do gateway.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: não

GatewayType

O tipo do gateway.

Tipo: sequências

Valores Válidos: `BACKUP_VM`

Obrigatório: não

HypervisorId

O ID do hipervisor do gateway.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Obrigatório: não

LastSeenTime

A última vez que o AWS Backup gateway se comunicou com o gateway, em formato Unix e horário UTC.

Tipo: carimbo de data/hora

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

GatewayDetails

Serviço: AWS Backup gateway

Os detalhes do gateway.

Conteúdo

GatewayArn

O Nome do recurso da Amazon (ARN) do gateway. Use a operação `ListGateways` para retornar uma lista de gateways para sua conta e Região da AWS.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Comprimento máximo de 180.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obrigatório: não

GatewayDisplayName

O nome de exibição do gateway.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: não

GatewayType

O tipo do tipo de gateway.

Tipo: sequências

Valores Válidos: `BACKUP_VM`

Obrigatório: não

HypervisorId

O ID do hipervisor do gateway.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Obrigatório: não

LastSeenTime

Detalhes mostrando a última vez que o AWS Backup gateway se comunicou com a nuvem, em formato Unix e horário UTC.

Tipo: carimbo de data/hora

Obrigatório: não

MaintenanceStartTime

Retorna a hora de início da manutenção semanal de gateway incluindo o dia da semana e a hora. Observe que os valores estão em termos do fuso horário do gateway. Pode ser semanal ou mensal.

Tipo: objeto MaintenanceStartTime

Obrigatório: Não

NextUpdateAvailabilityTime

Detalhes mostrando o horário de disponibilidade da próxima atualização do gateway.

Tipo: carimbo de data/hora

Obrigatório: não

VpcEndpoint

O nome DNS do endpoint da nuvem privada virtual (VPC) que o gateway usa para se conectar à nuvem para o gateway de backup.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 255.

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Hypervisor

Serviço: AWS Backup gateway

Representa as permissões do hipervisor ao qual o gateway se conectará.

Um hipervisor é um hardware, software ou firmware que cria e gerencia máquinas virtuais e aloca recursos para elas.

Conteúdo

Host

O host do servidor do hipervisor. Isso pode ser um endereço IP ou um nome de domínio totalmente qualificado (FQDN).

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 3. O tamanho máximo é 128.

Padrão: `^.+$`

Obrigatório: não

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obrigatório: não

KmsKeyArn

O Amazon Resource Name (ARN) do AWS Key Management Service usado para criptografar o hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Obrigatório: não

Name

O nome do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: não

State

O nome do hipervisor.

Tipo: sequências

Valores Válidos: `PENDING | ONLINE | OFFLINE | ERROR`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

HypervisorDetails

Serviço: AWS Backup gateway

Esses são os detalhes do hipervisor especificado. Um hipervisor é um hardware, software ou firmware que cria e gerencia máquinas virtuais e aloca recursos para elas.

Conteúdo

Host

O host do servidor do hipervisor. Isso pode ser um endereço IP ou um nome de domínio totalmente qualificado (FQDN).

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 3. O tamanho máximo é 128.

Padrão: `^.+$`

Obrigatório: não

HypervisorArn

O Nome do recurso da Amazon (ARN) do hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obrigatório: não

KmsKeyArn

O Nome do recurso da Amazon (ARN) do AWS KMS usado para criptografar o hipervisor.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Obrigatório: não

LastSuccessfulMetadataSyncTime

Esse é o momento em que ocorreu a sincronização com êxito mais recente dos metadados.

Tipo: carimbo de data/hora

Obrigatório: não

LatestMetadataSyncStatus

Esse é o status mais recente da sincronização de metadados indicada.

Tipo: sequências

Valores Válidos: `CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED`

Obrigatório: não

LatestMetadataSyncStatusMessage

Esse é o status mais recente da sincronização de metadados indicada.

Tipo: sequência

Obrigatório: não

LogGroupArn

O Nome do recurso da Amazon (ARN) do grupo de gateways no log solicitado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 0. Comprimento máximo de 2.048.

Padrão: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Obrigatório: não

Name

Esse é o nome do hipervisor especificado.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: não

State

Esse é o estado atual do hipervisor especificado.

Os estados possíveis são `PENDING`, `ONLINE`, `OFFLINE` ou `ERROR`.

Tipo: sequências

Valores Válidos: `PENDING | ONLINE | OFFLINE | ERROR`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

MaintenanceStartTime

Serviço: AWS Backup gateway

Essa e a hora de início da manutenção semanal de gateway incluindo o dia da semana e a hora. Observe que os valores estão em termos do fuso horário do gateway. Pode ser semanal ou mensal.

Conteúdo

HourOfDay

O componente de hora do horário de início da manutenção representado como hh, em que hh é a hora (0 a 23). A hora do dia está no fuso horário do gateway.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 23.

Obrigatório: Sim

MinuteOfHour

O componente de minuto do horário de início da manutenção representado como mm, em que mm é o minuto (0 a 59). O minuto da hora está no fuso horário do gateway.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 59.

Obrigatório: Sim

DayOfMonth

O componente dia do mês do horário de início da manutenção representado como um número ordinal de 1 a 28, em que 1 representa o primeiro dia do mês e 28 representa o último dia do mês.

Tipo: inteiro

Intervalo válido: valor mínimo de 1. Valor máximo de 31.

Obrigatório: não

DayOfWeek

Um número ordinal entre 0 e 6 que representa o dia da semana, em que 0 representa domingo e 6 representa sábado. O dia da semana está no fuso horário do gateway.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 6.

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Tag

Serviço: AWS Backup gateway

Um par de chave/valor que ajuda você a gerenciar, filtrar e pesquisar seus recursos. Os caracteres permitidos incluem letras UTF-8, números, espaços e os seguintes caracteres: + - = . _ : /.

Conteúdo

Key

A parte da chave do par de chave/valor da tag. A chave não pode começar com `aws:`.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. O tamanho máximo é 128.

Padrão: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Exigido: Sim

Value

A parte do valor do par de chave/valor da tag.

Tipo: sequência

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[^\x00]*$`

Exigido: Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

VirtualMachine

Serviço: AWS Backup gateway

Uma máquina virtual que está em um hipervisor.

Conteúdo

HostName

O nome do host da máquina virtual.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: não

HypervisorId

O ID do hipervisor da máquina virtual.

Tipo: sequência

Obrigatório: não

LastBackupDate

A data mais recente do backup de uma máquina virtual, em formato Unix e horário UTC.

Tipo: carimbo de data/hora

Obrigatório: não

Name

O nome da máquina virtual.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: não

Path

O caminho da máquina virtual.

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. O tamanho máximo é 4.096.

Padrão: `^[^\x00]+$`

Obrigatório: não

ResourceArn

O Nome do recurso da Amazon (ARN) da máquina virtual. Por exemplo, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

VirtualMachineDetails

Serviço: AWS Backup gateway

Seus objetos `VirtualMachine`, ordenados pelos seus Nomes de recurso da Amazon (ARNs).

Conteúdo

HostName

O nome do host da máquina virtual.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: não

HypervisorId

O ID do hipervisor da máquina virtual.

Tipo: sequência

Obrigatório: não

LastBackupDate

A data mais recente do backup de uma máquina virtual, em formato Unix e horário UTC.

Tipo: carimbo de data/hora

Obrigatório: não

Name

O nome da máquina virtual.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^[a-zA-Z0-9-]*$`

Obrigatório: não

Path

O caminho da máquina virtual.

Tipo: sequência

Restrições de Tamanho: Tamanho Mínimo 1. O tamanho máximo é 4.096.

Padrão: `^[^\x00]+$`

Obrigatório: não

ResourceArn

O Nome do recurso da Amazon (ARN) da máquina virtual. Por exemplo, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Tipo: sequência

Restrições de tamanho: tamanho mínimo de 50. Tamanho máximo de 500.

Padrão: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obrigatório: não

VmwareTags

Esses são os detalhes das tags da VMware associadas à máquina virtual especificada.

Tipo: matriz de objetos VmwareTag

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

VmwareTag

Serviço: AWS Backup gateway

Uma tag da VMware é uma tag anexada a uma máquina virtual específica. Uma tag é um par de chave/valor que ajuda você a gerenciar, filtrar e pesquisar seus recursos.

O conteúdo das tags da VMware pode ser combinado com as tags. AWS

Conteúdo

VmwareCategory

Essa é a categoria da VMware.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 80.

Obrigatório: não

VmwareTagDescription

Esse é o nome definido pelo usuário de uma tag da VMware.

Tipo: sequência

Obrigatório: não

VmwareTagName

Esse é o nome definido pelo usuário de uma tag da VMware.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 80.

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

VmwareToAwsTagMapping

Serviço: AWS Backup gateway

Isso exibe o mapeamento das tags VMware para as tags correspondentes AWS .

Conteúdo

AwsTagKey

A parte principal do par de AWS valores-chave da tag.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. O tamanho máximo é 128.

Padrão: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Exigido: Sim

AwsTagValue

A parte do valor do par de AWS valores-chave da tag.

Tipo: sequência

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[^\x00]*$`

Exigido: Sim

VmwareCategory

Essa é a categoria da VMware.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 80.

Obrigatório: Sim

VmwareTagName

Esse é o nome definido pelo usuário de uma tag da VMware.

Tipo: sequência

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 80.

Obrigatório: Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Parâmetros gerais

A lista a seguir contém os parâmetros que todas as ações usam para assinar solicitações do Signature versão 4 com uma string de consulta. Todos os parâmetros específicos de uma ação são listados no tópico para a ação. Para obter mais informações sobre o Signature versão 4, consulte Assinatura de solicitações de API da AWS no Guia do usuário do IAM.

Action

A ação a ser executada.

Tipo: string

Obrigatório: sim

Version

A versão da API para a qual a solicitação foi escrita, expressa no formato AAAA-MM-DD.

Tipo: string

Obrigatório: sim

X-Amz-Algorithm

O algoritmo de hash que foi usado para criar a assinatura da solicitação.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Valores válidos: `AWS4-HMAC-SHA256`

Obrigatório: Condicional

X-Amz-Credential

O valor de escopo da credencial, uma string que inclui a sua chave de acesso, a data, a região visada, o serviço que está sendo solicitado e uma sequência de encerramento ("aws4_request"). O valor é expresso no seguinte formato: chave_acesso/AAAAMMDD/região/serviço/aws4_request.

Para obter mais informações, consulte Criação de uma solicitação de API da AWS assinada no Guia do usuário do IAM.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Obrigatório: Condicional

X-Amz-Date

A data usada para criar a assinatura. O formato deve ser o formato básico ISO 8601 (AAAAMMDD'T'HHMMSS'Z'). Por exemplo, a data/hora a seguir é um valor X-Amz-Date válido: `20120325T120000Z`.

Condição: X-Amz-Date é opcional para todas as solicitações e pode ser usado para substituir a data usada para assinar solicitações. Se o cabeçalho Date (Data) for especificado no formato básico ISO 8601, o valor X-Amz-Date não será necessário. Quando X-Amz-Date é usado, sempre substitui o valor do cabeçalho Date (Data). Para obter mais informações, consulte Elementos de uma assinatura de solicitação de API da AWS no Guia do usuário do IAM.

Tipo: string

Obrigatório: Condicional

X-Amz-Security-Token

O token de segurança temporário que foi obtido por meio de uma chamada para o AWS Security Token Service (AWS STS). Para obter uma lista de serviços que oferecem suporte a credenciais de segurança temporárias do AWS STS, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Condição: se estiver usando credenciais de segurança temporárias do AWS STS, será necessário incluir o token de segurança.

Tipo: string

Obrigatório: Condicional

X-Amz-Signature

Especifica a assinatura com codificação hexadecimal que foi calculada com base na string a ser assinada e na chave de assinatura derivada.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Obrigatório: Condicional

X-Amz-SignedHeaders

Especifica todos os cabeçalhos HTTP que foram incluídos como parte da solicitação canônica. Para obter mais informações sobre a especificação de cabeçalhos assinados, consulte Criação de uma solicitação de API da AWS assinada no Guia do usuário do IAM.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Obrigatório: Condicional

Erros comuns

Esta seção lista os erros comuns às ações de API de todos os serviços da AWS. Para saber os erros específicos de uma ação de API para esse serviço, consulte o tópico sobre a ação de API em questão.

AccessDeniedException

Você não tem acesso suficiente para executar essa ação.

Código de status HTTP: 400

IncompleteSignature

A assinatura da solicitação não segue os padrões da AWS.

Código de status HTTP: 400

InternalFailure

O processamento da solicitação falhou por causa de um erro, uma exceção ou uma falha desconhecida.

Código de status HTTP: 500

InvalidAction

A ação ou operação solicitada é inválida. Verifique se a ação foi digitada corretamente.

Código de status HTTP: 400

InvalidClientTokenId

O certificado X.509 ou o ID de chave de acesso da AWS fornecido não existe em nossos registros.

Código de status HTTP: 403

NotAuthorized

Você não tem permissão para realizar esta ação.

Código de status HTTP: 400

OptInRequired

O ID da chave de acesso da AWS precisa de uma assinatura do serviço.

Código de status HTTP: 403

RequestExpired

A solicitação atingiu o serviço mais de 15 minutos após a data na solicitação ou mais de 15 minutos após a data de expiração da solicitação (como para URLs predeterminados), ou a data na solicitação está a mais de 15 minutos no futuro.

Código de status HTTP: 400

ServiceUnavailable

Falha na solicitação devido a um erro temporário do servidor.

Código de status HTTP: 503

ThrottlingException

A solicitação foi negada devido à limitação da solicitação.

Código de status HTTP: 400

ValidationError

A entrada não atende às restrições especificadas por um serviço da AWS.

Código de status HTTP: 400

Histórico do documento para AWS Backup

- Versão da API: 6 de dezembro de 2023
- Última atualização da documentação: 3 de junho de 2024

A tabela a seguir lista todos os AWS Backup lançamentos desde o lançamento do serviço em janeiro de 2019 até o presente. Para receber notificações sobre atualizações dessa documentação, assine um feed RSS acima.

Alteração	Descrição	Data
AWS Backup característica Expansão regional	AWS Backup o suporte ao nível de arquivamento de snapshots do Amazon EBS agora está disponível nas seguintes regiões: • China (Pequim) • China (Ningxia) • AWS GovCloud (Oeste dos EUA) • AWS GovCloud (Leste dos EUA)	3 de junho de 2024
Atualização das políticas gerenciadas pela AWS	AWS Backup adicionou permissão `backup:TagResource` às seguintes políticas gerenciadas: • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3Backup • AWSBackupServiceLinkedRolePolicyForBackup	17 de maio de 2024

Alteração	Descrição	Data
	Para obter mais informaçõ es, consulte Atualizações de políticas.	
AWS Backup agora disponíve l na região Oeste do Canadá (Calgary)	O backup e a restauração de vários tipos de recursos agora estão disponíveis no Oeste Região da AWS do Canadá (Calgary). Para recursos de backup compatíveis, consulte Disponibilidade de recursos por Região da AWS. Para ver os tipos de recursos compatíveis, consulte Serviços suportados por Região da AWS.	14 de março de 2024
Permissões adicionadas à política gerenciada	AWS Backup atualizou a política AWSServiceRolePoli cyForBackupRestore Testingadicionando permissõe s para oferecer suporte a outros tipos de recursos no recurso de teste de restauraç ão. Para obter mais informações sobre as permissões específic as adicionadas, consulte Atualizações de políticas.	14 de fevereiro de 2024

Alteração	Descrição	Data
Suporte de backup e restauração para FSx para volumes ONTAP FlexGroup	AWS Backup agora suporta backup e restauração de FSx para FlexGroup volumes ONTAP na maioria. Regiões da AWS Para obter mais informações, consulte Restoring an Amazon FSx file system. .	10 de janeiro de 2024
Suporte a backup e restauração de SAP HANA HA	AWS Backup agora oferece suporte a bancos de dados de alta disponibilidade SAP HANA no backup e restauração do Amazon EC2. Para obter mais informações, consulte SAP HANA on Amazon EC2 backups e Restoring an SAP HANA High Availability system.	21 de dezembro de 2023

Alteração	Descrição	Data
AWS Backup Controle do Audit Manager para testes de restauração	AWS Backup O Audit Manager agora oferece o controle do tempo de restauração para que os recursos atinjam a meta para auxiliar no monitoramento dos tempos de restauração. Esse controle verifica se o tempo de restauração de um recurso atende à duração desejada. Para obter mais informaçõ es, consulte Controles e remediação e Auditar testes de restauração.	18 de dezembro de 2023
Suporte ao armazenamento frio do Amazon EBS	AWS Backup agora suporta a transição de backups do EBS do armazenamento quente para o armazenamento frio. Para obter mais informações, consulte • Nível de arquivamento do Amazon EBS para armazenamento frio • Ciclo de vida e níveis de armazenamento • Criar um plano de backup	27 de novembro de 2023

Alteração	Descrição	Data
Apresentação do recurso de testes de restauração	AWS Backup introduz o teste de restauração, que traz uma avaliação automatizada e periódica da viabilidade da restauração, bem como a capacidade de monitorar os tempos de duração do trabalho de restauração. Para obter mais informações, consulte Testes de restauração.	27 de novembro de 2023

Alteração	Descrição	Data
Atualização das políticas gerenciadas pela AWS	AWS Backup adicionou as permissões `ec2:DescribeSnapshotTierStatus` e `ec2:ModifySnapshotTier` às políticas gerenciadas `AWSBackupServiceRolePolicyForBackups` `AWSBackupServiceLinkedRolePolicyForBackup` e. AWS Backup também adicionou as permissões `ec2:DescribeSnapshotTierStatus` e `ec2:RestoreSnapshotTier` a política gerenciada `AWSBackupServiceRolePolicyForRestores` . Essas permissões são necessárias para que os usuários tenham a opção de fazer a transição dos recursos do Amazon EBS armazenados AWS Backup para o armazenamento de arquivos e restaurar recursos do nível de armazenamento de arquivos. Para obter mais informações, consulte Policy updates.	27 de novembro de 2023

Alteração	Descrição	Data
Adição da permissão para enviar perfil a fim de oferecer suporte aos testes de restauração.	AWS Backup adicionado `restore-testing.backup.amazonaws.com` a `IamPassRolePermissions` `IamCreateServiceLinkedRolePermissions` e. Essa adição é necessária AWS Backup para realizar testes de restauração em nome dos clientes.	27 de novembro de 2023

Alteração	Descrição	Data
Adição de um novo perfil vinculado ao serviço.	AWS Backup adicionou a nova função vinculada ao serviço chamada `AWSServiceRoleForBackupRestoreTesting`, que fornece permissões de backup para realizar testes de restauração. Essa nova função vinculada ao serviço AWS Backup fornece as permissões necessárias para realizar testes de restauração. As permissões incluem as ações `list, read, and write` para que os seguintes serviços sejam incluídos nos testes de restauração: 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 e Amazon S3.	27 de novembro de 2023

Alteração	Descrição	Data
Novo painel de métricas de trabalho no AWS Backup console	O AWS Backup console agora exibe um painel de tarefas, simplificando o monitoramento da integridade do backup em grande escala com uma nova interface visual de usuário e métricas agregadas de backup, cópia e restauração para serviços suportados pela. AWS Backup O painel de empregos está disponível em todas as regiões em que o AWS Backup Audit Manager está disponível. As regiões não listadas ainda poderão acessar o CloudWatch painel. Para obter mais informações, consulte AWS Backup console dashboards.	15 de novembro de 2023

Alteração	Descrição	Data
Compatibilidade com backups de pilha aninhada	AWS Backup expandiu seu suporte para backups de AWS CloudFormation recursos. Suas pilhas de CloudFormation aplicativos que têm pilhas aninhadas dentro delas podem ser incluídas em seus backups. Para obter mais informações, consulte Backups de pilha do CloudFormation .	8 de novembro de 2023
Compatibilidade com o Amazon S3 nas regiões China (Pequim) e China (Ningxia).	AWS Backup o suporte para o Amazon S3 agora está disponível nas regiões da China (Pequim) e China (Ningxia). Para obter mais informações, consulte Disponibilidade de recursos por região.	26 de outubro de 2023
Support para backups contínuos e restauração P do Amazon Aurora oint-in-time	AWS Backup agora oferece suporte a backups e point-in-time restauração contínuos (PITR) para recursos do Aurora. Para obter mais informações, consulte Backups contínuos e oint-in-time recuperação de P.	7 de setembro de 2023

Alteração	Descrição	Data
AWS CloudFormation as pilhas suportam a exclusão de recursos	AWS Backup agora oferece suporte à opção de excluir os recursos escolhidos da sua AWS CloudFormation pilha. Para obter mais informações, consulte Backups de pilha do AWS CloudFormation.	6 de setembro de 2023
As regras do plano de backup apresentam a flexibilidade de fuso horário	AWS Backup as regras do plano agora podem ter um fuso horário específico para janelas de backup. Para obter mais informações, consulte Gerenciar planos de backup.	28 de agosto de 2023
AWS Backup agora disponível na região de Israel (Tel Aviv)	Muitos AWS Backup recursos agora estão disponíveis na nova região de Israel (Tel Aviv). Para ver quais recursos são compatíveis, acesse Disponibilidade de recursos por Região da AWS.	22 de agosto de 2023

Alteração	Descrição	Data
AWS Backup O Audit Manager agora oferece suporte a contas de administrador delegado	AWS Backup A geração de relatórios do Audit Manager agora pode ser acessada por contas de administrador delegado. Para obter mais informações, consulte • Audite backups e crie relatórios com o AWS Backup Audit Manager • Trabalhar com relatórios de auditoria • Administrador delegado	16 de agosto de 2023
Pré-visualizar cofre de backup logicamente isolado	AWS Backup agora oferece uma prévia de um novo tipo de cofre de backup para ajudar a complementar as operações de proteção de dados. Para obter mais informações, consulte Cofres logicamente isolados (pré-visualização).	8 de agosto de 2023
AWS Backup aprimora os backups do Amazon S3	AWS Backup aumentou os recursos de desempenho, tamanho e velocidade para backups de bucket do S3. Para obter mais informações, consulte Backups do Amazon S3.	1º de agosto de 2023

Alteração	Descrição	Data
O recurso Tag na restauração agora está disponível nas regiões da China	Agora, as tags que fazem parte de um backup podem ser copiadas ao criar um trabalho de restauração nas regiões China (Pequim) ou China (Ningxia). Para obter mais informações, consulte Copiar tags durante uma restauração.	17 de julho de 2023
AWS Backup agora oferece suporte ao Amazon S3 em regiões adicionais	AWS Backup O suporte para o Amazon S3 agora está disponível nas regiões da Europa (Espanha), Europa (Zurique), Ásia-Pacífico (Hyderabad) e Ásia-Pacífico (Melbourne). Para obter mais informações, consulte Disponibilidade de recursos por região.	6 de julho de 2023

Alteração	Descrição	Data
A cópia entre contas foi expandida para regiões adicionais	AWS Backup agora oferece suporte à cópia de backup entre contas da maioria dos recursos nas seguintes regiões: Ásia-Pacífico (Jacarta), Oriente Médio (Bahrein), Ásia-Pacífico (Hong Kong), África (Cidade do Cabo), Europa (Milão), Ásia-Pacífico (Osaka), Oriente Médio (Emirados Árabes Unidos), Europa (Espanha), Europa (Zurique), Ásia-Pacífico (Hyderabad) e Ásia-Pacífico (Melbourne). Para obter mais informações consulte Disponibilidade de recursos por região.	5 de julho de 2023
Backup Audit Manager disponível em GovCloud regiões	AWS Backup expandiu o AWS Backup Audit Manager para AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA). Para obter mais informações, consulte Disponibilidade de recursos por região.	29 de junho de 2023

Alteração	Descrição	Data
O gerenciamento de várias contas agora está disponível nas regiões GovCloud	AWS Backup agora oferece suporte ao gerenciamento de recursos entre contas em AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA). Para obter mais informações, consulte Gerenciar recursos do AWS Backup em várias contas da AWS.	29 de junho de 2023
Compatibilidade com cópias entre regiões do Amazon Aurora em regiões adicionais	AWS Backup agora oferece suporte a cópias de backup entre regiões para clusters Aurora de e para as seguintes regiões: Ásia-Pacífico (Jacarta), Oriente Médio (Bahrein), Ásia-Pacífico (Hong Kong), África (Cidade do Cabo), Europa (Milão), Oriente Médio (Emirados Árabes Unidos), Europa (Espanha), Europa (Zurique), Ásia-Pacífico (Hyderabad) e Ásia-Pacífico (Melbourne).	5 de junho de 2023
Copiar tags durante a restauração	As tags que fazem parte de um backup agora poderão ser copiadas quando você criar uma tarefa de restauração. Para obter mais informações, consulte Copiar tags durante uma restauração.	22 de maio de 2023

Alteração	Descrição	Data
AWS Backup integra-se às notificações AWS do usuário	Agora você pode optar por receber notificações relacionadas a eventos de backup, cópia e restauração por meio do console de notificações do usuário da AWS. Para obter mais informações, consulte Introdução às notificações AWS do usuário.	10 de maio de 2023
Backups entre regiões disponíveis em quatro novas regiões	AWS Backup agora oferece suporte ao backup entre regiões na região do Oriente Médio (EAU), na região da Europa (Espanha), na região da Europa (Zurique) e na região Ásia-Pacífico (Hyderabad).	28 de abril de 2023
Suporte expandido para AWS Backup cópias entre regiões	Agora, os backups entre regiões dos recursos do Amazon EFS, da VMware e do DynamoDB podem ser realizados nas seguintes regiões: Ásia-Pacífico (Jacarta), Oriente Médio (Bahrein), Ásia-Pacífico (Hong Kong), África (Cidade do Cabo) e Europa (Milão).	28 de abril de 2023

Alteração	Descrição	Data
Backup e restauração do Amazon S3 na região América do Sul (São Paulo)	AWS Backup o suporte para o Amazon S3 (Amazon Simple Storage Service) agora está disponível na região da América do Sul (São Paulo). Para obter mais informações, consulte Backups do Amazon S3.	20 de abril de 2023
AWS Backup expande-se para a região Ásia-Pacífico (Melbourne)	AWS Backup agora está disponível na região Ásia-Pacífico (Melbourne). Para obter mais informações, consulte Disponibilidade de recursos por AWS região.	20 de abril de 2023
Compatibilidade regional expandida para o Amazon S3	AWS Backup o suporte para o Amazon S3 (Amazon Simple Storage Service) agora está disponível nas regiões (Leste dos EUA) e AWS GovCloud AWS GovCloud (Oeste dos EUA) Para obter mais informações, consulte Backups do Amazon S3.	19 de abril de 2023

Alteração	Descrição	Data
Fazer backup e restaurar bancos de dados SAP HANA em instâncias do Amazon EC2	AWS Backup agora oferece a capacidade de fazer backup e restaurar bancos de dados SAP HANA executados em instâncias do Amazon EC2 na maioria das regiões. Para obter mais informações, consulte Bancos de dados SAP HANA no backup de instâncias do Amazon EC2.	17 de abril de 2023
AWS Backup agora disponível nas regiões da Europa (Espanha), Europa (Zurique) e Ásia-Pacífico (Hyderabad)	AWS Backup o suporte se expandiu para novas regiões, incluindo Europa (Espanha), Europa (Zurique) e Ásia-Pacífico (Hyderabad). É possível fazer o backup e a restauração dos recursos compatíveis nessas regiões. Para obter mais informações, consulte Disponibilidade de recursos por AWS região.	13 de abril de 2023

Alteração	Descrição	Data
Política AWS gerenciada atualizada `AWSBackupAuditAccess`	Política AWS gerenciada atualizada AWSBackupAuditAccess. AWS Backup substituiu a seleção de recursos na API `config:DescribeComplianceByConfigRule` por um recurso curinga. Para obter mais informações, consulte Atualizações de políticas para o AWS Backup.	11 de abril de 2023
Hipervisores com Amazon Logs CloudWatch	AWS Backup Agora, os usuários do gateway podem integrar hipervisores com o CloudWatch Logs para manter os registros. Para obter mais informações, consulte Edição de uma configuração de hipervisor e CloudWatch registros.	29 de março de 2023
Compatibilidade regional expandida para o Amazon S3	AWS Backup o suporte para o Amazon S3 agora está disponível nas regiões Ásia-Pacífico (Jacarta) e Oriente Médio (EAU).	22 de março de 2023

Alteração	Descrição	Data
Melhoria do backup incremental da máquina virtual	Os backups de VMs (máquinas virtuais) da VMware que apresentam problemas de dados CBT (Changed Block Tracking) agora contêm informações adicionais para ajudar a remediar e solucionar problemas. Para obter mais informações, consulte Backups incrementais de VM e Solução de problemas em suas máquinas virtuais.	15 de março de 2023
AWS Backup suporte para vários adaptadores de rede	AWS Backup o gateway agora suporta a configuração de vários adaptadores de rede Para obter mais informações sobre como configurar adaptadores de rede, consulte Configurar seu gateway para várias NICs na VMware no Guia do desenvolvedor do AWS Backup .	8 de março de 2023

Alteração	Descrição	Data
AWS Backup suporte para vSphere 8	AWS Backup agora suporta backup e restauração de máquinas virtuais que são executadas no VMware vSphere 8. Para obter mais informações sobre as opções compatíve is da VMware, consulte VMs compatíveis no Guia do desenvolvedor do AWS Backup .	8 de março de 2023
AWS Backup O Audit Manager é compatível com backups Multi-AZ do Amazon RDS	O Backup Audit Manager agora é compatível com backups Multi-AZ do Amazon Relational Database Service. Para obter mais informaçõ es, consulte como auditar backups e criar relatórios com o AWS Backup Audit Manager.	1° de fevereiro de 2023

Alteração	Descrição	Data
AWS Backup oferece backup incremental para tabelas do Amazon Timestream	AWS Backup agora oferece recursos de backup expandidos para backups do Timestream. Os planos de backup agora podem fazer backups incrementais para reduzir o tempo necessário para fazer backup dos recursos do Timestream e reduzir os custos de armazenamento. Para obter mais informações, consulte Backups do Amazon Timestream.	23 de janeiro de 2023
AWS Backup agora disponível em Dubai	AWS Backup expandiu-se para a região do Oriente Médio (EAU). É possível fazer backup e restauração dos recursos compatíveis nessa região.	17 de janeiro de 2023

Alteração	Descrição	Data
Cópia entre regiões disponível em regiões adicionais	AWS Backup agora oferece backups entre regiões na região Ásia-Pacífico (Jacarta) , no Oriente Médio (Bahrein), na região Ásia-Pacífico (Hong Kong), na região da África (Cidade do Cabo) e na região da Europa (Milão) para a maioria dos recursos. Para obter mais informaçõ es, consulte Criar cópias de backup entre Regiões da AWS.	21 de dezembro de 2022
Limites de largura de banda e controle de utilização do Backup Gateway	AWS Backup O gateway agora permite limites na taxa de transferência de upload dos gateways para controlar AWS Backup a quantidade de largura de banda de rede usada pelo gateway. Para oferecer suporte a esse recurso, AWS Backup criou e atualizou políticas gerenciad as, incluindo `AWSBackup FullAccess` `AWSBackup OperatorAccess` e. Para obter mais informações, consulte Controle de utilizaçã o de largura de banda do Backup Gateway.	15 de dezembro de 2022

Alteração	Descrição	Data
Compatibilidade com a tag da VMware do Backup Gateway	AWS Backup O Gateway agora oferece suporte a tags VMware. Os usuários têm a flexibilidade adicional de criar AWS tags que correspondam às tags usadas em máquinas virtuais. Para oferecer suporte a esse recurso, AWS Backup criou e atualizou políticas gerenciadas `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` `AWSBackupFullAccess` , incluindo , `AWSBackupOperatorAccess` e. Para obter mais informações, consulte Tags da VMware.	15 de dezembro de 2022
AWS Backup suporte para Amazon Timestream	AWS Backup agora oferece suporte ao backup e à restauração de tabelas do Amazon Timestream. Para obter mais informações, consulte Backup do Amazon Timestream.	13 de dezembro de 2022

Alteração	Descrição	Data
AWS Backup oferece Legal Hold	AWS Backup apresenta uma nova ferramenta para ajudar a proteger os pontos de recuperação por meio de uma retenção legal. Para obter mais informações, consulte Retenção legal.	27 de novembro de 2022
AWS Backup Audit Manager Relatórios entre regiões e contas	AWS Backup O Audit Manager traz funcionalidades adicionais aos relatórios de conformidade e de trabalho. Os usuários podem gerar relatórios incorporando várias regiões e contas. Para obter mais informaçõ es, consulte Trabalhar com relatórios de auditoria.	27 de novembro de 2022
AWS Backup oferece suporte ao Amazon Redshift	AWS Backup agora oferece suporte para fazer backup de clusters do Amazon Redshift e restaurar clusters e tabelas do Amazon Redshift. Para obter mais informações, consulte Backups do Amazon Redshift.	27 de novembro de 2022

Alteração	Descrição	Data
AWS Backup oferece suporte para pilhas de AWS CloudFormation aplicativos de backup	AWS Backup fornece a capacidade de fazer backup CloudFormation e restaurar aplicativos contendo vários recursos fazendo backup de uma pilha e restaurando os recursos dentro dela. Para obter mais informações, consulte Backups de pilha de aplicações.	27 de novembro de 2022
AWS Backup oferece contas delegadas de administrador e delegação de políticas de backup	AWS Backup as contas inscritas AWS Organizations podem designar contas de membros como contas de administrador delegado. Para obter mais informações, consulte Gerenciando várias contas com AWS Organizations.	27 de novembro de 2022

Alteração	Descrição	Data
Pré-visualização pública do SAP HANA no backup e restauração de instâncias do Amazon EC2	AWS Backup e a AWS Backint estão oferecendo uma prévia pública integrada da funcionalidade para backup e restauração de bancos de dados SAP HANA em instâncias EC2. Para obter mais informações, consulte nossa Pré-visualização pública do SAP HANA em instâncias do Amazon EC2. Para apoiar essa prévia, AWS Backup forneceu atualizações de políticas e novas políticas AWS gerenciadas para esses recursos.	20 de novembro de 2022
Restaurar a VMware em instâncias do Amazon EC2	AWS Backup agora oferece a capacidade de restaurar máquinas virtuais em instâncias do Amazon EC2, além da capacidade de restaurar máquinas para EBS, VMware, VMware Cloud on e VMware Cloud on. AWS AWS Outposts Para obter mais informações, consulte a documentação sobre como usar o AWS Backup console para restaurar os pontos de recuperação da máquina virtual.	9 de novembro de 2022

Alteração	Descrição	Data
Funcionalidade expandida AWS Backup do Vault Lock	AWS Backup O Vault Lock agora pode ser criado no modo de governança para proteções adicionais do IAM ou no modo de conformidade para garantir a imutabilidade. Saiba mais em AWS Backup Vault Lock.	04 de outubro de 2022
AWS Backup Audit Manager agora disponível na região da África (Cidade do Cabo) e na região da Europa (Milão)	AWS Backup O Audit Manager se expandiu para a região da África (Cidade do Cabo) e a região da Europa (Milão). Para obter mais informações sobre o Backup Audit Manager, consulte Auditar backups e criar relatórios com o AWS Backup Audit Manager.	14 de setembro de 2022
AWS Backup traz CloudWatch métricas da Amazon para o painel do console do Backup	AWS Backup aprimora o painel do console Backup para exibir CloudWatch métricas integradas da Amazon para trabalhos de backup e restauração, oferecendo capacidade e flexibilidade adicionais de monitoramento.	8 de setembro de 2022
Compatibilidade com a flexibilidade adicional de criptografia do Amazon EBS durante a restauração	AWS Backup agora oferece opções adicionais de criptografia durante a restauração dos snapshots do Amazon EBS.	1º de setembro de 2022

Alteração	Descrição	Data
AWS Backup oferece suporte à cópia de backup entre contas e regiões do Amazon S3	AWS Backup agora oferece cópia de backup entre regiões e entre contas para backups do Amazon S3. Para obter mais informações, consulte Backups do Amazon S3.	28 de julho de 2022
AWS Backup O Audit Manager oferece suporte de controle adicional para FSx for ONTAP	AWS Backup O Audit Manager agora oferece controles adicionais para apoiar o monitoramento e a auditoria de volumes FSx for ONTAP, incluindo recursos de backup protegidos por um plano de backup e pelo último ponto de recuperação criado. Para obter mais informaçõ es, consulte Controles e correções do AWS Backup Audit Manager.	22 de julho de 2022
AWS Backup adiciona suporte para backup e restauração de clusters Multi-AZ do Amazon RDS para clusters PostgreSQ L e MySQL	AWS Backup adicionou uma opção de backup e restauraç ão de cluster de zona de disponibilidade múltipla com uma instância de banco de dados primária e duas instâncias de banco de dados em espera legíveis. Para saber mais, consulte Backups Multi-AZ do Amazon RDS.	20 de julho de 2022

Alteração	Descrição	Data
AWS Backup O Audit Manager adiciona um novo controle para a criação de pontos de recuperação	AWS Backup O Audit Manager oferece um novo controle de auditoria para maior suporte à conformidade. `Last recovery point created` é um controle adicional opcional para garantir que os pontos de recuperação sejam criados dentro de prazos especific ados. Para saber mais, consulte Controle do último ponto de recuperação criado.	29 de junho de 2022
Amostra de endpoint de AWS Backup gateway adicionada	AWS Backup O Gateway forneceu um endpoint de amostra para ajudar os usuários a se conectarem a VPNs (Redes Privadas Virtuais). Para obter mais informações, consulte Criação de um AWS Backup VPC endpoint.	14 de junho de 2022

Alteração	Descrição	Data
AWS Backup agora oferece endpoints Amazon VPC para VMware	AWS Backup agora oferece suporte a endpoints Amazon VPC para VMware, permitindo que você use uma rede privada virtual entre seus ambientes VMware e o uso. AWS AWS PrivateLink Para obter mais informações, consulte Criar um gateway e AWS Backup e AWS PrivateLink.	1º de junho de 2022
AWS Backup O Audit Manager oferece suporte de controle adicional para o Amazon S3	O Backup Audit Manager agora oferece compatibilidade com o controle de conformidade Recursos de backup protegidos pelo plano de backup para tipos de recursos do S3. Para obter mais informações, consulte Controles e correções do AWS Backup Audit Manager.	25 de maio de 2022

Alteração	Descrição	Data
AWS Backup O Audit Manager oferece suporte de controle adicional para o Storage Gateway	O Backup Audit Manager agora oferece compatibilidade com o controle de conformidade Recursos de backup protegidos pelo plano de backup para tipos de recursos do Storage Gateway. Para obter mais informações, consulte Controles e correções do AWS Backup Audit Manager.	25 de maio de 2022
Compatibilidade com o Amazon FSx para OpenZFS	AWS Backup agora oferece gerenciamento adicional de proteção de dados para backup e restauração no FSx para sistemas de arquivos OpenZFS.	18 de maio de 2022
AWS Backup Suporte do Audit Manager para VMware	AWS Backup agora fornece suporte para máquinas virtuais nos controles e remediação do Backup Audit Manager. Para obter mais informações, consulte Controles e correções do AWS Backup Audit Manager.	11 de maio de 2022
O Amazon FSx para Lustre agora está disponível na região Ásia-Pacífico (Osaka).	AWS Backup agora oferece backup do Amazon FSx na região Ásia-Pacífico (Osaka) e cópias entre regiões de e para a região Ásia-Pacífico (Osaka).	26 de abril de 2022

Alteração	Descrição	Data
Compatibilidade com Persistent_2 do Amazon FSx para Lustre	AWS Backup agora oferece disponibilidade geral de suporte para o Amazon FSx for Lustre, que suporta níveis mais altos de taxa de transferência por unidade de armazenamento em comparação aos sistemas de arquivos Persistent_1.	5 de abril de 2022
Aprimoramentos à VMware	AWS Backup agora oferece restauração para o volume do Amazon EBS, restauração em nível de disco e suporte para VMware on. AWS Outposts Para obter mais informaçõ es, consulte Restaurar uma máquina virtual.	31 de março de 2022
AWS Backup Disponibilidade para Ásia-Pacífico (Jacarta)	AWS Backup agora está disponível para clientes na região Ásia-Pacífico (Jacarta).	17 de março de 2022
Novos controles para o AWS Backup Audit Manager	AWS Backup O Audit Manager apresenta três novos controles de auditoria: cópia entre regiões, cópia entre contas e Backup Vault Lock. Para obter mais informaçõ es, consulte Controles e correções do AWS Backup Au dit Manager.	17 de março de 2022

Alteração	Descrição	Data
Support for AWS PrivateLink	Com AWS PrivateLink o for AWS Backup, você pode se conectar diretamente AWS Backup usando um endpoint de interface em sua VPC em vez de se conectar pela Internet pública. Os endpoints de interface podem ser acessados diretamente a partir de aplicativos que estão no local ou em uma AWS região diferente. Para obter mais informações, consulte AWS Backup e AWS PrivateLink.	28 de fevereiro de 2022
Compatibilidade com o Amazon Simple Storage Service (Amazon S3)	A disponibilidade geral do AWS Backup Amazon S3 em geral Regiões da AWS está disponível, exceto nas regiões da China (Pequim), China (Ningxia), (Oeste dos EUA) e AWS GovCloud AWS GovCloud (Leste dos EUA). Para obter mais informações, consulte Trabalhar com dados do Amazon S3.	14 de fevereiro de 2022
Support para backup avançado do DynamoDB nas regiões da China AWS	O backup avançado do DynamoDB já está disponível nas regiões China (Pequim) e China (Ningxia). Para obter mais informações, consulte Backup avançado do DynamoDB.	18 de janeiro de 2022

Alteração	Descrição	Data
Pré-visualização pública do Amazon S3	AWS Backup oferece uma prévia pública dos backups do Amazon S3. Para ter mais informações, consulte Trabalhar com dados do Amazon S3.	30 de novembro de 2021
Compatibilidade com máquinas virtuais (VMs) da VMware	Agora você pode usar AWS Backup para fazer backup automático de VMs VMware. Para ter mais informaçõ es, consulte Backups de máquinas virtuais.	30 de novembro de 2021
Compatibilidade com o backup avançado do DynamoDB	Agora você pode usar AWS Backup para executar os seguintes recursos em todos os novos backups de tabelas do DynamoDB que você criar: armazenamento em camadas, marcação de alocação de custos, cópia entre regiões, cópia entre contas, criptogra fia independente e cópia de tags das tabelas de origem do DynamoDB. Para obter mais informações, consulte Backup avançado do DynamoDB o Guia do desenvolvedor do Amazon DynamoDB e Como usar AWS Backup com o DynamoDB.	23 de novembro de 2021

Alteração	Descrição	Data
Support para aprimoramento da atribuição de AWS Backup recursos nas regiões da China AWS	AWS Backup o aprimoramento da atribuição de recursos agora está disponível na região da China (Pequim) e na região da China (Ningxia). Para obter mais informações, consulte Atribuir recursos a um plano de backup.	16 de novembro de 2021
Lançamento do aprimoramento da atribuição de AWS Backup recursos	O aprimoramento da atribuição de recursos de backup oferece controles adicionais e refinados e novos processos simplificados para implantar planos de backup que protegem centenas de milhares de recursos. AWS Use esse recurso para aumentar a velocidade, flexibilidade e precisão ao proteger os dados usando o AWS Backup. Para obter mais informações, consulte Atribuir recursos a um plano de backup.	10 de novembro de 2021
Compatibilidade com o Amazon Neptune	Agora você pode usar AWS Backup para fazer backup dos clusters do Amazon Neptune. Para saber mais, consulte O que é o AWS Backup?	5 de novembro de 2021

Alteração	Descrição	Data
Compatibilidade com o Amazon DocumentDB	Agora você pode usar AWS Backup para fazer backup dos clusters do Amazon DocumentDB. Para saber mais, consulte O que é o AWS Backup?	5 de novembro de 2021
Support para o AWS Backup Vault Lock nas regiões AWS da China	AWS Backup O Vault Lock agora está disponível na região da China (Pequim) e na região da China (Ningxia). Para obter mais informações, consulte Vault Lock do AWS Backup.	3 de novembro de 2021
Lançamento do AWS Backup Vault Lock	Com o AWS Backup Vault Lock, você pode impedir a exclusão de backups armazenados em um cofre de AWS Backup backup. Para obter mais informações, consulte Vault Lock do AWS Backup.	7 de outubro de 2021
Lançamento dos relatórios de conformidade do AWS Backup Audit Manager	Com relatórios de conformidade, você pode gerar relatórios diários sobre a conformidade de suas atividades e recursos de backup em relação aos controles definidos nas estruturas do AWS Backup Audit Manager. Para obter mais informações, consulte Modelos de relatórios de conformidade.	5 de outubro de 2021

Alteração	Descrição	Data
AWS CloudFormation suporte para AWS Backup Audit Manager	Com AWS CloudFormation, agora você pode implantar estruturas, controles e planos de relatórios do AWS Backup Audit Manager de forma segura e repetível em grande escala. Para obter mais informações, consulte Auditoria e relatórios de backup com o AWS Backup Audit Manager.	4 de outubro de 2021
Lançamento do AWS Backup Audit Manager	Com o AWS Backup Audit Manager, agora você pode definir controles para sua atividade e recursos de backup e identificar as atividades e os recursos que não estão em conformidade com seus controles. Você também pode usar o AWS Backup Audit Manager para gerar relatórios diários e sob demanda que servem como evidência da conformidade com seus controles definidos ao longo do tempo. Para obter mais informações, consulte Auditoria e relatórios de backup com o AWS Backup Audit Manager.	24 de agosto de 2021

Alteração	Descrição	Data
Compatibilidade com novas operações assíncronas de pontos de recuperação	AWS Backup agora assume uma função vinculada ao serviço para gerenciar suas regras de ciclo de vida de backup caso você tenha modificado ou excluído sua função original do IAM. Para obter mais informações, consulte Excluir backups.	23 de agosto de 2021
Compatibilidade com backups consistentes em caso de falha para vários volumes do Amazon EBS.	Agora, quando você usa AWS Backup para proteger suas instâncias do Amazon EC2, AWS Backup faz backups de vários volumes e consistentes com falhas de todos os volumes do Amazon EBS anexados a cada instância do Amazon EC2 por padrão. Para obter mais informações, consulte Criar backup consistente em caso de falha de vários volumes do Amazon EBS.	14 de junho de 2021

Alteração	Descrição	Data
Support para Amazon FSx, além de Regiões da AWS	Agora você pode usar AWS Backup para proteger seus sistemas de arquivos Amazon FSx nas seguintes regiões: região da Europa (Milão) AWS GovCloud (US), região da África (Cidade do Cabo) e região do Oriente Médio (Bahrein). Para obter mais informações, consulte Endpoints e cotas do AWS Backup, na Referência geral da AWS .	15 de abril de 2021
Compatibilidade com backups entre contas do Amazon FSx	Agora você pode usar AWS Backup para copiar backups Regiões da AWS e contas do Amazon FSx. Para obter mais informações, consulte Criar uma cópia de backup. Se usar políticas gerenciadas pelo cliente, você deverá adicionar a nova permissão `fsx:CopyBackup` para evitar que haja falha nos trabalhos de backup existentes. Para obter essa permissão, consulte a última instrução na política de backup do Amazon FSx nas Políticas gerenciadas pelo cliente.	12 de abril de 2021

Alteração	Descrição	Data
Compatibilidade com as tags de alocação de custos para backups do Amazon EFS	Agora você pode usar tags de alocação de custos para rastrear os custos de seus backups do Amazon EFS em um nível detalhado e visualizar e filtrar essas tags usando AWS Cost Explorer. Para obter mais informaçõ es, consulte Usar tags de alocação de custos.	7 de abril de 2021
Autorização FedRAMP High	AWS Backup agora está autorizada a oferecer suporte às cargas de trabalho do FedRAMP High. Para obter mais informações, consulte Serviços da AWS no escopo por programa de conformid ade.	25 de março de 2021
Novo Região da AWS	AWS Backup agora está disponível na região Ásia-Pací fico (Osaka). Nessa região, o AWS Backup atualmente não é compatível com o Storage Gateway, o Amazon FSx e backup entre contas. Para obter mais informações, consulte Endpoints e cotas do AWS Backup, na Referência geral da AWS .	25 de março de 2021

Alteração	Descrição	Data
Compatibilidade com operações em lote de pontos de recuperação	Agora você pode usar o AWS Backup console para automatizar as operações em lote para limpar os pontos de recuperação em seus cofres de backup. Para obter mais informações, consulte Excluir backups.	23 de março de 2021
Compatibilidade com restaurações na classe de armazenamento One Zone do Amazon EFS	Agora você pode restaurar seus backups do Amazon EFS para a classe de armazenamento One Zone do Amazon EFS. Para obter mais informações, consulte Restaurar um sistema de arquivos do Amazon EFS.	12 de março de 2021
Support para restauração e backup contínuo do Amazon Relational Database point-in-time Service	Agora você pode usar AWS Backup para automatizar backups contínuos e realizar point-in-time restaurações (PITR) do Amazon RDS, além de orquestrar seus backups de snapshots. Para obter mais informações, consulte Restaurando em um horário especificado usando a point-in-time recuperação.	10 de março de 2021

Alteração	Descrição	Data
Support para Amazon CloudWatch	Agora você pode usar CloudWatch para monitorar AWS Backup métricas. Para obter mais informações, consulte Monitoramento de eventos e métricas com a Amazon CloudWatch e a Amazon EventBridge.	3 de fevereiro de 2021
Support para Amazon EventBridge	Agora você pode usar EventBridge para monitorar AWS Backup eventos. Para obter mais informações, consulte Monitoramento de eventos e métricas com a Amazon CloudWatch e a Amazon EventBridge.	3 de fevereiro de 2021
Compatibilidade com backups entre contas	Agora você pode usar AWS Backup para fazer backup de seus recursos em vários Contas da AWS. Para obter mais informações, consulte Criação de cópias de backup em várias AWS contas.	18 de novembro de 2020
Compatibilidade com sistemas de backup do Amazon FSx	Agora você pode usar AWS Backup para fazer backup dos sistemas de arquivos Amazon FSx. Para obter mais informações, consulte Trabalhar com armazenamento e sistemas de arquivos do Amazon FSx.	9 de novembro de 2020

Alteração	Descrição	Data
Novo Regiões da AWS	AWS Backup agora está disponível na África (Cidade do Cabo) e na Europa (Milão) Regiões da AWS. Para obter mais informações, consulte Endpoints e cotas do AWS Backup, na Referência geral da AWS .	21 de outubro de 2020
Compatibilidade com o backup do Windows habilitado para VSS	Agora é possível fazer backup e restaurar aplicações do Windows compatíveis com VSS (Serviço de Cópias de Sombra de Volume) em instâncias do Amazon EC2. Para obter mais informaçõ es, consulte Criar backups de VSS do Windows.	22 de setembro de 2020
Compatibilidade com o backup automático do Amazon EFS	Agora você pode usar AWS Backup para fazer backup automático dos sistemas de arquivos do Amazon EFS. Para obter mais informações, consulte Conceitos básicos 4: Criar backups automáticos do Amazon EFS.	16 de julho de 2020
Novo Região da AWS	AWS Backup agora está disponível no AWS GovCloud (US) Region. Para obter mais informações, consulte Endpoints e cotas do AWS Backup, na Referência geral da AWS .	24 de junho de 2020

Alteração	Descrição	Data
Support para gerenciar backups em vários Contas da AWS	Agora você pode gerenciar backups em vários Contas da AWS usando AWS Organizations. Para obter mais informações, consulte Como funciona o gerenciamento entre contas.	24 de junho de 2020
Support para Amazon Aurora adicionado ao AWS Backup	Agora você pode configurar AWS Backup para fazer backup de recursos para o Amazon Aurora. Para obter informações, consulte Visão geral de backup e restauração de um cluster de banco de dados do Aurora no Guia do usuário do Amazon Aurora.	10 de junho de 2020
Support para configurar serviços com os quais trabalhar AWS Backup	Agora você pode configurar AWS Backup para fazer backup de recursos para AWS serviços específicos. Para obter mais informações, consulte Aceitar o gerenciamento de serviços com AWS Backup.	20 de maio de 2020
Compatibilidade com o backup de instâncias do Amazon EC2 e também a adição da compatibilidade com para backups entre regiões.	Agora é possível fazer backup de instâncias inteiras do Amazon EC2 e também copiar recursos entre Regiões da AWS. Para obter mais informações, consulte Criar cópias de backup entre Regiões da AWS.	13 de janeiro de 2020

Alteração	Descrição	Data
Novo guia	AWS lançamentos AWS Backup e o Guia do AWS Backup Desenvolvedor.	15 de janeiro de 2019

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.