
AWS Backup

Guia do desenvolvedor



AWS Backup: Guia do desenvolvedor

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

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o AWS Backup?	1
Compatível com recursos e aplicativos de terceiros	1
Recursos e regiões compatíveis	1
Visão geral do AWS Backup	3
Gerenciamento centralizado de backups	4
Backup com base em políticas	4
Políticas de backup baseadas em tag	4
Políticas de gerenciamento de vida	4
Backups incrementais	4
Backup entre regiões	4
Gerenciamento entre contas e backup entre contas	5
Monitorar atividades de backup	5
Proteja seus dados em cofres de backup	5
Satisfazer as obrigações	6
Conceitos básicos	6
Como funcionam	7
Trabalhar com outros serviços	7
Aceitar a gestão de serviços com AWS Backup	7
Trabalho com sistemas de arquivos do Amazon FSx	8
Trabalhar com o Amazon EC2	8
Trabalhar com o Amazon EFS	9
Trabalhar com o Amazon DynamoDB	10
Trabalhar com o Amazon EBS	10
Trabalho com o Amazon RDS e o Amazon Aurora	10
Trabalhar com o AWS Storage Gateway	10
Como os serviços fazem backup de seus próprios recursos	11
Medição de backup e uso de preços	11
Blogs, vídeos, tutoriais e outros recursos	11
Configuração	14
Cadastro na AWS	14
Criar um usuário do IAM	14
Criar uma função do IAM	16
Conceitos básicos	17
Prerequisites	17
Opção 1: Criar um backup sob demanda	18
Próximas etapas	19
Opção 2: Criar um backup agendado	19
Etapa 1: Para criar um plano de backup modificando um plano existente	20
Etapa 2: Atribuir recursos a um plano de backup	20
Etapa 3: Criar um cofre de backup	21
Próximas etapas	22
Opção 3: Criar backups automáticos do Amazon EFS	22
Monitore os trabalhos de backup	23
Exibir o status dos trabalhos de backup	23
Exibir todos os backups em um cofre	24
Exibir detalhes dos recursos protegidos	24
Próximas etapas	24
Restaurar um backup	24
Próximas etapas	25
Limpar os recursos	26
Etapa 1: Excluir restaurado AWS recursos	26
Etapa 2: Excluir o plano de backup	26
Etapa 3: Excluir os pontos de recuperação	26
Etapa 4: Excluir o cofre de backup	27

Gerenciar planos de backup	28
Como criar um plano de backup	28
Criando planos de backup usando oAWS Management Console	28
Opções e configuração do plano de backup	29
Atribuir recursos	32
Excluir um plano de backup	33
Atualizar um plano de backup	33
Trabalhar com cofres de backup	35
Como criar um cofre de backup	35
Nome do cofre de backup	35
Chave de criptografia do KMS	35
Tag do cofre de backup	36
Definindo políticas de acesso em cofres de backup e pontos de recuperação	36
Negar acesso a um tipo de recurso em um cofre de backup	36
Negar acesso a um cofre de backup	37
Negar acesso a excluir pontos de recuperação em um cofre de backup	37
Excluir um cofre de backup	39
Trabalhar com backups	40
Criar um backup	41
Backups sob demanda	42
Recuperação point-in-time	43
Criando backups do Windows VSS	47
Como criar backups consistentes com falhas e multivolume do Amazon EBS	48
Copiar tags em backups	48
Interromper um trabalho de backup	49
Copiar um backup	49
Backup entre regiões	49
Backups entre contas	51
Visualizar uma lista de backups	59
Listando backups por recurso protegido	59
Listando backups por cofre de backup	60
Editar um backup	60
Restaurar um backup	61
Restaurar um sistema de arquivos do Amazon FSx	61
Restaurar um volume do EBS	65
Restaurar um sistema de arquivos EFS	66
Restaurar um banco de dados do DynamoDB	69
Restaurar um banco de dados do Amazon RDS	70
Restaurar um cluster do Aurora	72
Restaurar uma instância do EC2	74
Restaurar umaAWS Storage Gatewayvolume	76
Usar oAWS BackupAPI, CLI ou SDK para restaurar pontos de recuperação do Amazon EC2	76
Gerenciando backups em várias contas com Organizations	77
Criando uma conta de Gerenciamento em Organizations	78
Como habilitar o gerenciamento entre contas	78
Como criar uma política de backup	78
Monitoramento de atividades em váriasAWScontas	82
Regras de inclusão de recursos	82
Definição de políticas, sintaxe de políticas e herança de políticas	82
O uso doAWS CloudFormationModelos comAWS Backup	84
Em geral	84
O uso doAWS CloudFormationAutomatizarAWS BackupCom o Windows VSS	86
O uso doAWS CloudFormationCom Organizations	86
Segurança	93
Proteção de dados	93
Criptografia para backups noAWS	94
Identity and Access Management	97

Authentication	98
Controle de acesso	99
Funções de serviço IAM	103
Políticas gerenciadas	104
Funções vinculadas ao serviço	160
Atualizações da política	162
Validação de conformidade	165
Resiliência	166
Segurança da infraestrutura	167
Cotas	168
Monitoramento	169
MonitoramentoAWS BackupEventos usando o EventBridge	169
Monitorar eventos usando o EventBridge	169
Diferenças com oAWS BackupAPI de notificação	190
MonitoramentoAWS Backupmétricas com o CloudWatch	191
Monitore métricas com o CloudWatch	191
Diferenças com oAWS Backuppainel	193
Registro em logAWS BackupChamadas de API com CloudTrail	193
AWS BackupInformações do no CloudTrail	194
Noções básicas sobre entradas de arquivos de log do AWS Backup	195
Registrar em log eventos de gerenciamento	197
Uso do Amazon SNS para rastrear eventos	199
Configurando o console do Amazon SNS	199
AWS BackupAPIs de notificação	200
Exemplos de eventos	200
AWS BackupExemplos de comandos de	202
EspecificandoAWS BackupComo um principal de serviço	203
Solução de problemas do AWS Backup	205
Solução de problemas gerais	205
Solução de problemas de criação	205
Solução de problemas de exclusão	206
API do AWS Backup	207
Actions	207
CreateBackupPlan	209
CreateBackupSelection	213
CreateBackupVault	216
DeleteBackupPlan	219
DeleteBackupSelection	222
DeleteBackupVault	224
DeleteBackupVaultAccessPolicy	226
DeleteBackupVaultNotifications	228
DeleteRecoveryPoint	230
DescribeBackupJob	232
DescribeBackupVault	237
DescribeCopyJob	240
DescribeGlobalSettings	242
DescribeProtectedResource	244
DescribeRecoveryPoint	246
DescribeRegionSettings	251
DescribeRestoreJob	253
DisassociateRecoveryPoint	257
ExportBackupPlanTemplate	259
GetBackupPlan	261
GetBackupPlanFromJSON	265
GetBackupPlanFromTemplate	268
GetBackupSelection	271
GetBackupVaultAccessPolicy	274

GetBackupVaultNotifications	276
GetRecoveryPointRestoreMetadata	279
GetSupportedResourceTypes	282
ListBackupJobs	284
ListBackupPlans	287
ListBackupPlanTemplates	290
ListBackupPlanVersions	292
ListBackupSelections	295
ListBackupVaults	298
ListCopyJobs	300
ListProtectedResources	303
ListRecoveryPointsByBackupVault	305
ListRecoveryPointsByResource	308
ListRestoreJobs	311
ListTags	314
PutBackupVaultAccessPolicy	317
PutBackupVaultNotifications	319
StartBackupJob	322
StartCopyJob	326
StartRestoreJob	330
StopBackupJob	333
TagResource	335
UntagResource	337
UpdateBackupPlan	339
UpdateGlobalSettings	343
UpdateRecoveryPointLifecycle	345
UpdateRegionSettings	349
Tipos de dados	350
AdvancedBackupSetting	352
BackupJob	354
BackupPlan	358
BackupPlanInput	359
BackupPlansListMember	360
BackupPlanTemplatesListMember	362
BackupRule	363
BackupRuleInput	365
BackupSelection	367
BackupSelectionsListMember	368
BackupVaultListMember	370
CalculatedLifecycle	372
Condition	373
CopyAction	374
CopyJob	375
Lifecycle	378
ProtectedResource	379
RecoveryPointByBackupVault	380
RecoveryPointByResource	383
RecoveryPointCreator	385
RestoreJobsListMember	386
Erros comuns	388
AWSGlossário	390
Histórico do documento	391
.....	CCCXCV

O que é o AWS Backup?

AWS Backup é um serviço de proteção de dados totalmente gerenciado que facilita a centralização e a automação entre AWS serviços, na nuvem e no local. Usando este serviço, você pode configurar políticas de backup e monitorar a atividade do seu AWS recursos em um só lugar. Ele permite que você automatize e consolide tarefas de backup que foram anteriormente realizadas serviço por serviço e remove a necessidade de criar scripts personalizados e processos manuais. Com alguns cliques no AWS Backup Console, você pode automatizar suas políticas e agendas de proteção de dados.

AWS Backup não controla os backups que você faz no seu AWS Ambiente fora do AWS Backup. Portanto, se você quiser uma solução centralizada e completa para requisitos de conformidade normativa e de negócios, comece a usar AWS Backup Hoje.

Compatível AWS Recursos e aplicativos de terceiros

Os seguintes exemplos de AWS Recursos e aplicativos de terceiros dos quais você pode fazer backup e restaurar usando o AWS Backup.

Serviço compatível	Recurso compatível
Amazon FSx	Sistemas de arquivos do Amazon FSx
Amazon Elastic File System (Amazon EFS)	Sistemas de arquivos do Amazon EFS
Amazon DynamoDB	Tabelas do DynamoDB
Amazon Elastic Compute Cloud (Amazon EC2)	Instâncias do Amazon EC2 (excluindo instâncias compatíveis com o armazenamento)
Windows VSS (Serviço de Cópia de Sombra de Volume)	Aplicativos compatíveis com Windows VSS (incluindo Windows Server e Microsoft SQL Server) no Amazon EC2
Amazon Elastic Block Store (Amazon EBS)	Volumes do Amazon EBS
Amazon Relational Database Service (Amazon RDS)	Bancos de dados Amazon RDS (incluindo todos os mecanismos de banco de dados)
Amazon Aurora	Clusters Aurora
AWS Storage Gateway (Gateway de volume)	AWS Storage Gateway Volumes do

Recursos e regiões compatíveis

AWS Backup oferece os seguintes recursos em TODOS os compatíveis AWS Serviços e aplicativos de terceiros.

- Programações de backup automatizadas e gerenciamento de retenção
- [Monitoramento centralizado de backups](#)

- [Criptografia de backup integrada ao KMS](#)
- [Backup entre regiões](#)
- [Gerenciamento entre contas](#)
- [Backup entre contas](#)

AWS Backup **SOMENTE** oferece os seguintes recursos com esses compatíveis AWS Serviços da .

- Ciclo de vida para armazenamento frio e restauração em nível de item com o Amazon EFS
- [Backup contínuo e restauração point-in-time com Amazon RDS \(exceto Aurora\)](#)

AWS Backup **NÃO** oferece as seguintes combinações de serviço de recurso.

- O DynamoDB e o Aurora não oferecem suporte a backup incremental. Cada backup feito é um backup completo.
- O DynamoDB não oferece suporte a backup entre regiões. O DynamoDB também não oferece suporte a backup entre contas.
- O Amazon RDS e o Aurora não oferecem suporte a backup entre regiões E entre contas como uma única ação de cópia. Você pode escolher um ou outro. Você também pode usar um AWS Lambda para escutar quando a primeira cópia for concluída, execute a segunda cópia e exclua a primeira cópia.

AWS Backup está disponível em todas as seguintes AWS Regiões. Este gráfico também mostra quais recursos não estão disponíveis em uma determinada região.

AWS Backup Suporte	Backup entre regiões	Gerenciamento entre contas	Backup entre contas	AWS Storage Gateway e o Amazon FSx
South America (São Paulo) Region	✓	✓	✓	✓
Asia Pacific (Sydney) Region	✓	✓	✓	✓
Asia Pacific (Tokyo) Region	✓	✓	✓	✓
Europe (Ireland) Region	✓	✓	✓	✓
US East (Ohio) Region	✓	✓	✓	✓
Região Europa (Londres)	✓	✓	✓	✓
US West (Oregon) Region	✓	✓	✓	✓
US West (N. California) Region	✓	✓	✓	✓
Asia Pacific (Mumbai) Region	✓	✓	✓	✓

AWS BackupSuporte	Backup entre regiões	Gerenciamento entre contas	Backup entre contas	AWS Storage Gatewaye o Amazon FSx
Região Europa (Paris)	✓	✓	✓	✓
Região Europa (Estocolmo)	✓	✓	✓	✓
Asia Pacific (Singapore) Region	✓	✓	✓	✓
Região do Canadá (Central)	✓	✓	✓	✓
Asia Pacific (Seoul) Region	✓	✓	✓	✓
US East (N. Virginia) Region	✓	✓	✓	✓
Europe (Frankfurt) Region	✓	✓	✓	✓
Região China (Pequim)	✓			✓
Região China (Ningxia)	✓			✓
Middle East (Bahrain) Region				✓
Região Ásia-Pacífico (Hong Kong)				✓
Africa (Cape Town) Region				✓
Europe (Milan) Region				✓
Região da Ásia-Pacífico (Osaka)	✓	✓		
AWSGovCloud (Oeste dos EUA)	✓		✓	✓
AWSGovCloud (Leste dos EUA)	✓		✓	✓

Visão geral do AWS Backup

O AWS Backup fornece os seguintes recursos e funcionalidades.

Gerenciamento centralizado de backups

O 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 no AWS que seus aplicativos usam. Com o AWS Backup, você pode gerenciar centralmente as políticas de backup que atendem aos seus requisitos de backup. Em seguida, você pode aplicá-las ao seu AWS recursos no AWS. Com o, você pode fazer o backup de dados de aplicativo de uma maneira consistente e compatível. O console de backup centralizado do AWS Backup oferece uma visão consolidada dos seus backups e logs de atividades de backup, facilitando a auditoria de backup e garantindo a conformidade.

Backup com base em políticas

Com o AWS Backup, é possível criar políticas de backup conhecidas como planos de backup. Use esses planos de backup para definir seus requisitos de backup e as aplique ao AWS recursos que você deseja proteger no AWS. Os serviços da que você usar. 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 é submetido a backup 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.

Políticas de backup baseadas em tag

Você pode usar o AWS Backup para aplicar planos de backup ao seu AWS, marcando-os. A marcação facilita implementar sua estratégia de backup em todos os seus aplicativos e a garantir que todos os seus AWS são armazenados em backup e protegidos. As tags são uma maneira excelente de organizar e classificar seu AWS recursos da AWS. Integração do com o AWS permite que você aplique rapidamente um plano de backup a um grupo de AWS para que o backup seja feito de forma consistente e compatível.

Políticas de gerenciamento de vida

O AWS Backup permite que você atenda aos requisitos de conformidade e reduza os custos de armazenamento de backups com o armazenamento de backups em um nível de armazenamento "frio" e econômico. 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.

Atualmente, apenas os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio". A expressão de armazenamento "frio" é ignorada para os backups do Amazon EBS, Amazon RDS, Amazon Aurora, Amazon DynamoDB e AWS Storage Gateway.

Backups incrementais

O AWS Backup armazena eficientemente seus backups periódicos incrementalmente. O primeiro backup de um AWS faz backup de uma cópia completa dos seus dados. Para cada backup incremental sucessivo, somente as alterações em seu AWS recursos são armazenados em backup. Os backups incrementais permitem que você se beneficie da proteção de dados de backups frequentes, minimizando os custos de armazenamento.

Atualmente, o DynamoDB e o Aurora não oferecem suporte a backup incremental. Cada backup periódico do DynamoDB ou do Aurora é uma cópia completa dos seus dados.

Backup entre regiões

O uso do AWS Backup, você pode copiar backups para vários AWS Regiões sob demanda ou automaticamente como parte de um plano de backup programado. 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 [Criação de cópias de backup em AWS Regiões da](#).

Gerenciamento entre contas e backup entre contas

Você pode usar AWS Backup para gerenciar seus backups em todas as AWS Contas dentro do [AWS Organizations](#) Estrutura. Com o gerenciamento entre contas, é possível usar automaticamente políticas de backup para aplicar planos de backup no AWS Contas dentro da 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 o AWS Backup recursos em várias AWS Contas](#).

Você também pode copiar backups em várias AWS Contas dentro do AWS Organizations Estrutura de gestão. Dessa forma, você pode “ventilar” backups em uma única conta de repositório e, em seguida, “liberar” backups para maior resiliência. [Criação de cópias de backup em AWS Contas](#).

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

Monitorar atividades de backup

AWS Backup O fornece um painel que simplifica a auditoria de atividades de backup e restauração entre AWS Serviços da . Com apenas alguns cliques no console do AWS Backup, você pode visualizar o status dos trabalhos de backup recentes. Você também pode restaurar trabalhos em AWS para garantir que seu AWS estão devidamente protegidos.

AWS Backup integra-se ao Amazon CloudWatch e ao Amazon EventBridge. O CloudWatch permite rastrear métricas e criar alarmes. EventBridge permite que você visualize e monitore AWS Backup. Para obter mais informações, consulte [Monitoramento AWS Backup Eventos usando o EventBridge](#) e [Monitoramento AWS Backup métricas com o CloudWatch](#).

AWS Backup O integra-se ao AWS CloudTrail. O CloudTrail fornece uma visão consolidada dos logs de atividades de backup que facilitam e agilizam a auditoria de como o backup de seus recursos é feito. AWS Backup O 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 em log AWS Backup Chamadas de API com CloudTrail](#) e [Usando o Amazon SNS para rastrear AWS Backup Eventos do](#).

Proteja seus dados em cofres de backup

AWS Backup armazena seus backups em cofres de backup, que os separa com segurança de suas instâncias de origem. Por exemplo, seu cofre manterá seus backups do Amazon EC2 e do Amazon EBS de acordo com a política de ciclo de vida escolhida, mesmo se você excluir a instância do Amazon EC2 de origem e os volumes do Amazon EBS.

Os cofres de backup oferecem políticas de acesso baseadas em recursos e criptografia que permitem definir 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 AWS, ajudando você a atender aos seus requisitos de conformidade. Para revisar AWS Políticas gerenciadas pelo cliente para o AWS Backup, consulte <https://docs.aws.amazon.com/aws-backup/latest/devguide/security-iam-awsmanpol.html>.

Satisfazer as obrigações

AWS Backup ajuda você a estatificar suas obrigações globais de conformidade. AWS Backup está no escopo dos seguintes exemplos de AWS Programas de conformidade:

- [Alto do FedRAMP](#)
- [GDPR](#)
- [SOC 1, 2 e 3](#)
- [PCI](#)
- [HIPAA](#)
- [E muito mais](#)

Conceitos básicos

Para saber mais a respeito AWS Backup Recomendamos começar com [Conceitos básicos do AWS Backup](#) (p. 17).

AWS Backup: Como funcionam

AWS Backup é um serviço de backup totalmente gerenciado que facilita a centralização e a automação do backup de dados no AWS. Com o AWS Backup, você pode criar políticas de backup conhecidas como 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 ao seu AWS simplesmente marcando-os. AWS Backup em seguida, faz automaticamente o backup do AWS Recursos de acordo com o plano de backup que você definiu.

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

Tópicos

- [Como AWS Backup Trabalhar com outros AWS Serviços da](#) (p. 7)
- [Medição de backup e uso de preços](#) (p. 11)
- [AWS Backup blogs, vídeos, tutoriais e outros recursos](#) (p. 11)

Como AWS Backup Trabalhar com outros AWS Serviços da

Alguns AWS oferecem seus próprios recursos de backup, incluindo snapshots do Amazon Elastic Block Store (Amazon EBS), snapshots do Amazon Relational Database Service (Amazon RDS), backups do Amazon DynamoDB, AWS Storage Gateway instantâneos e outros. Esses recursos estão disponíveis para você independentemente de você usar AWS Backup.

Para configurar o AWS Backup para gerenciar centralmente os backups dos serviços suportados, você deve optar por gerenciar esse serviço com o AWS Backup, inicie seus backups usando AWS Backup e armazene seus backups em cofres de backup. No entanto, os backups de outros AWS não estão disponíveis para governança central por meio do AWS Backup.

Tópicos

- [Aceitar a gestão de serviços com AWS Backup](#) (p. 7)
- [Trabalho com sistemas de arquivos do Amazon FSx](#) (p. 8)
- [Trabalhar com o Amazon EC2](#) (p. 8)
- [Trabalhar com o Amazon EFS](#) (p. 9)
- [Trabalhar com o Amazon DynamoDB](#) (p. 10)
- [Trabalhar com o Amazon EBS](#) (p. 10)
- [Trabalho com o Amazon RDS e o Amazon Aurora](#) (p. 10)
- [Trabalhar com o AWS Storage Gateway](#) (p. 10)
- [Como AWS serviços fazem backup de seus próprios recursos](#) (p. 11)

Aceitar a gestão de serviços com AWS Backup

Quando novo AWS se tornarem disponíveis, você deverá habilitar o AWS Backup para usar esses serviços. Se você tentar criar um backup sob demanda ou um plano de backup usando recursos de um serviço que não está habilitado, você receberá uma mensagem de erro e não poderá concluir o processo.

Note

As configurações de inclusão de serviços são específicas da região. Se você alterar o `AWSRegião` que você está usando, reconfigure os serviços que você usa com o AWS Backup.

Para configurar os serviços usados com o AWS Backup

1. Abrir o AWS Backup no <https://console.aws.amazon.com/backup>.
2. No painel de navegação, selecione Settings.
3. Na página Optar pela adoção do serviço, escolha Configurar recursos. Use os botões de alternância para habilitar ou desabilitar os serviços usados com o AWS Backup.
4. Escolha Confirmar quando os serviços estiverem configurados.

Note

Backups criados com AWS Backup não pode ser excluído usando APIs que pertencem ao recurso submetido a backup. Para obter informações sobre como excluir pontos de recuperação usando a API do AWS Backup, consulte [DeleteRecoveryPoint](#) (p. 230).

Trabalho com 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, como armazenamento baseado no Microsoft Windows, computação de alto desempenho, aprendizado de máquina e automação de design eletrônico.

O Amazon FSx oferece suporte a dois tipos de sistema de arquivos: Lustre e Windows File Server. Você pode fazer backup de qualquer sistema de arquivos do Amazon FSx for Windows File Server e de qualquer sistema de arquivos do Amazon FSx for Lustre que tenha armazenamento persistente e que não esteja vinculado a um repositório de dados como o Amazon S3. AWS Backup usa a funcionalidade de backup interna do Amazon FSx. Assim, os backups retirados do AWS Backup têm o mesmo nível de consistência e desempenho do sistema de arquivos e as mesmas opções de restauração que os backups que são feitos por meio do console do Amazon FSx.

Se você usar o AWS Backup para gerenciar esses backups, você obtém funcionalidades adicionais, como opções de retenção ilimitadas, e a capacidade de criar backups agendados com a frequência de cada hora. Além disso, AWS Backup mantém seus backups mesmo após o sistema de arquivos de origem ser excluído. Isso protege contra exclusão acidental ou maliciosa.

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

- Como fazer backup de recursos: [Conceitos básicos do AWS Backup](#) (p. 17)
- Como restaurar recursos do Amazon FSx: [Restaure um sistema de arquivos do Amazon FSx](#) (p. 61)

Para obter informações detalhadas sobre sistemas de arquivos do Amazon FSx, consulte o [Documentação do Amazon FSx](#).

Trabalhar com o Amazon EC2

O uso do AWS Backup, você pode programar ou executar trabalhos de backup sob demanda que incluem instâncias do EC2 inteiras e aplicativos do Windows executados no Amazon EC2, juntamente com dados de configuração associados. Isso limita a necessidade de interação com o volume de armazenamento (Amazon EBS). Da mesma forma, você pode restaurar uma instância do Amazon EC2 a partir de um

único ponto de recuperação. Um trabalho de backup pode ter apenas um recurso. Assim, você pode ter um trabalho para fazer backup de uma instância do EC2, e ele fará backup do volume raiz, de todos os volumes de dados e das configurações de instância associadas.

AWS Backup não reinicializa instâncias do EC2 a qualquer momento.

Backup de recursos do Amazon EC2

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

Você também pode fazer backup e restaurar seus aplicativos do Microsoft Windows habilitados para VSS. Você pode programar backups consistentes com aplicativos, definir políticas de ciclo de vida e executar restaurações consistentes como parte de um backup sob demanda ou de um plano de backup agendado. Para obter mais informações, consulte [Criando backups do Windows VSS](#) (p. 47).

AWS Backup não faz backup do seguinte:

- Configuração do acelerador Elastic Inference, se ele estiver anexado à instância.
- Dados do usuário usados quando a instância foi iniciada.

Note

Para todos os tipos de instância, somente as instâncias do EC2 baseadas no Amazon EBS são compatíveis. Instâncias de armazenamento temporário (ou seja, instâncias baseadas em armazenamento de instância) não são compatíveis.

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

Um snapshot deriva sua criptografia do volume conforme definido por você, e a mesma criptografia é aplicada aos snapshots correspondentes. Os snapshots do EBS de uma AMI copiada serão sempre criptografados. Se você usar uma chave do KMS durante a cópia, a chave será aplicada. Se você não usar uma chave do KMS, uma chave padrão do KMS será aplicada.

- Como fazer backup de recursos: [Conceitos básicos do AWS Backup](#) (p. 17)
- Como restaurar recursos do Amazon EC2: [Restaurar uma instância do Amazon EC2](#) (p. 74)

Para obter informações detalhadas sobre o Amazon EC2, consulte [O que é o Amazon EC2?](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Trabalhar com o Amazon EFS

O AWS Backup atualmente oferece suporte ao Amazon Elastic File System (Amazon EFS).

- Como fazer backup de recursos: [Conceitos básicos do AWS Backup](#) (p. 17)
- Como restaurar recursos do Amazon EFS: [Restaurar um sistema de arquivos do Amazon EFS](#) (p. 66)

Para obter informações detalhadas sobre 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 DynamoDB

AWS Backup atualmente oferece suporte ao Amazon DynamoDB (DynamoDB).

- Como fazer backup de recursos: [Conceitos básicos do AWS Backup](#) (p. 17)
- Como restaurar recursos do DynamoDB: [Restaurando um banco de dados do Amazon DynamoDB](#) (p. 69)

Para obter informações detalhadas sobre o DynamoDB, consulte [O que é o Amazon DynamoDB?](#) no Guia do desenvolvedor do Amazon DynamoDB.

Trabalhar com o Amazon EBS

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

- Como fazer backup de recursos: [Conceitos básicos do AWS Backup](#) (p. 17)
- Como restaurar volumes do Amazon EBS: [O uso do AWS Backup Para restaurar um volume do Amazon EBS](#) (p. 65)

Para obter informações detalhadas sobre volumes do Amazon EBS consulte [O que é o Amazon Elastic Block Store \(Amazon EBS\)?](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Para obter mais informações, consulte [Como criar um volume do Amazon EBS](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Trabalho com o Amazon RDS e o Amazon Aurora

AWS Backup atualmente suporta mecanismos de banco de dados do Amazon RDS e clusters do Aurora.

- Como fazer backup de recursos: [Conceitos básicos do AWS Backup](#) (p. 17)
- Como restaurar recursos do Amazon RDS: [Restaurar um banco de dados do Amazon RDS](#) (p. 70)
- Como restaurar clusters do Amazon Aurora: [Restaure um cluster do Amazon Aurora](#) (p. 72)

Para obter mais informações sobre o Amazon RDS, consulte [O que é o Amazon Relational Database Service?](#) no Amazon RDS User Guide.

Para obter informações detalhadas sobre o Aurora, consulte [O que é o Amazon Aurora?](#) no Amazon Aurora Guia do usuário.

Note

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 Trabalho de backup expirado antes da conclusão. Se isso ocorrer, configure uma janela de backup mais longa no AWS Backup.

Trabalhar com o AWS Storage Gateway

Os snapshots do Amazon EBS podem ser restaurados como o AWS Storage Gateway Volumes do.

- Como fazer backup de recursos: [Conceitos básicos do AWS Backup](#) (p. 17)

Para obter informações detalhadas sobre o AWS Storage Gateway, consulte [O que é o AWS Storage Gateway?](#) no AWS Storage Gateway Guia do usuário do.

Como AWS serviços fazem backup de seus próprios recursos

Para obter informações sobre como usar o AWS para fazer backup de seus recursos, consulte o seguinte:

- [Amazon EC2 Related Services](#)
- [O uso do AWS Backup com 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](#)
- [O uso do AWS Backup com o Amazon FSx for Windows File Server](#)
- [O uso do AWS Backup com Amazon FSx for Lustre](#)
- [Fazer backup de seus volumes no AWS Storage Gateway](#)

Medição de backup e uso de preços

O uso de backup para recursos de backup existentes (exceto o Amazon EFS) continuará a ser medido e cobrado por seus respectivos serviços, e a definição de preço permanece inalterada. Não há custo adicional para usar o AWS Backup recursos de backup centralizado além dos preços existentes de armazenamento de backup cobrados pelo AWS, como taxas de armazenamento de snapshots do Amazon EBS. Não há cobrança adicional pelos backups de instâncias do Amazon EC2.

Para serviços que introduzem AWS Backup- Recursos nativos, como o Amazon EFS, o uso de backup é medido e cobrado por AWS Backup. Para obter mais informações, consulte [Definição de preço do AWS Backup](#).

Você pode usar tags de alocação de custos para controlar custos de seus backups do Amazon EFS em um nível detalhado, e visualizar e filtrar essas tags usando o AWS Cost Explorer. Para obter mais informações, consulte [Automatização de backups e otimização dos custos de backup para o Amazon EFS usando AWS Backup](#) e [Usar tags de alocação de custos](#).

Important

Para evitar cobranças adicionais, configure sua política de retenção com uma duração de armazenamento quente de pelo menos uma semana. AWS Backup calcula seu ciclo de vida a partir do início do trabalho de backup, não da conclusão. Por exemplo, suponha que você faça backups diários e os mantenha por um dia. Suponha ainda que seus recursos protegidos sejam tão grandes que leva o dia inteiro para concluir o backup. AWS Backup implementará o período de rentabilidade de um dia e removerá o backup do armazenamento quente quando o trabalho de backup for concluído. No dia seguinte, AWS Backup não pode criar um backup incremental porque não há backup no armazenamento quente. 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. Peça orientação ao seu gerente técnico de conta ou arquiteto de soluções sobre seu caso de uso.

AWS Backup blogs, vídeos, tutoriais e outros recursos

Para obter mais informações sobre AWS Backup veja o seguinte:

- [Automatize o backup centralizado em escala em AWS Serviços que usam o AWS Backup](#). Com Ibukun Oyewumi e Sabith Venkitachalapathy (julho de 2021).
- [Como simplificar o backup do Microsoft SQL Server usando AWS Backup 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).
- [Configurar notificações para monitorar o AWS Backup trabalhos](#). Com Virgil Ennes (junho de 2021).
- [Publicações no blog Automatização de backups e otimização dos custos de backup para o Amazon EFS usando AWS Backup](#). Com Prachi Gupta e Rohit Verma (junho de 2021).
- [Gerenciar custos de backup do Amazon EFS: AWS Backup Suporte para tags de alocação de custos](#). Com Aditya Maruvada (maio 2021).
- [Publicações no blog Crie e compartilhe backups criptografados entre contas e regiões usando AWS Backup](#). Com Prachi Gupta (maio de 2021).
- [Publicações no blog AWS Backup agora é aprovado pelo FedRAMP High para suas necessidades de conformidade e proteção de dados](#). Com Andy Grimes (maio de 2021).
- [Publicações no blog A ZS Associates aumenta 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 o AWS Backup](#). Com Fathima Kamal (abril de 2021).
- [Tutoriais do vídeo Gerenciamento de cópias de backups entre regiões](#). Com David DeLuca (abril de 2021).
- [Publicações no blog Excluir vários AWS Backup Pontos de recuperação usando o AWS Tools for PowerShell](#). Com Sherif Talaat (abril de 2021).
- [Publicações no blog Backups entre regiões e entre contas do Amazon FSx usando o AWS Backup](#). Com Adam Hunter e Fathima Kamal (abril de 2021).
- [Publicações no blog Eventos e métricas do Amazon CloudWatch para o AWS Backup](#). Com Rolland Miller (março de 2021).
- [Tutorial: Backup e restauração do Amazon Relational Database Service \(RDS\) usando o AWS Backup](#). Com Fathima Kamal (março de 2021).
- [Publicações no blog Recuperação point-in-time e backup contínuo para o Amazon RDS com o AWS Backup](#). Com Kelly Griffin (março de 2021).
- [Publicações no blog Automatizar o AWS Backup por AWS Catálogo de serviços](#). Com John Husemoller (janeiro de 2021).
- [Publicações no blog Recuperação segura de dados com backup entre contas e cópia entre regiões usando AWS Backup](#). Com Cher Simon (janeiro de 2021).
- [Publicações no blog AWS Recapitulação do re:Invent: Proteção de dados e conformidade com AWS Backup](#). Com Nancy Wang (dezembro de 2020).
- [Publicações no blog AWS Backup fornece proteção centralizada de dados em toda a sua AWS recursos](#). Com Nancy Wang (novembro de 2020).
- [Conversa técnica: Proteção de dados em escala com AWS Backup](#). Com Kareem Behairy (setembro de 2020).
- [Publicações no blog Gerenciamento centralizado entre contas com cópia entre regiões usando AWS Backup](#). Com Cher Simon (setembro de 2020).
- [Tutoriais do vídeo Gerenciando backups em escala em seu AWS Organizations usando AWS Backup](#). Com Ildar Sharafiev (julho de 2020).
- [Publicações no blog Gerenciando backups em escala em seu AWS Organizations usando AWS Backup](#). Com Nancy Wang, Avi Drabkin, Ganesh Sundaresan e Vikas Shah (junho de 2020).
- [Publicações no blog Recupere arquivos e pastas do Amazon EFS com AWS Backup](#). Com Abrar Hussain e Gurudath Pai (maio 2020).
- [Publicações no blog Agendamento de backups automatizados usando o Amazon EFS e AWS Backup](#). Com Rob Barnes (dezembro de 2019).

- [Gravações re:Invent:AWSRe:Invent 2019: Mergulho profundoAWS Backupft Rackspace](#). Com Nancy Wang e Jason Pavao (dezembro de 2019).
- [Publicações no blog Proteger seus dados com oAWS Backup](#). Com Anthony Fiore (julho de 2019).
- [Vídeo de marketing: Apresentação doAWS Backup](#). Janeiro de 2019.
- [Vídeo: Introdução ao AWS Backup](#). comAWSTraining and Certification.

Configuração

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

1. [Cadastro na AWS](#) (p. 14)
2. [Criar um usuário do IAM](#) (p. 14)
3. [Criar uma função do IAM](#) (p. 16)

Cadastro na AWS

Quando você se cadastrar na Amazon Web Services (AWS), sua conta da AWS é automaticamente cadastrada em todos os serviços do AWS, incluindo AWS Backup. Você será cobrado apenas pelos serviços que usar.

Para obter mais informações sobre AWS Backup, consulte as [tarifas de utilização](#) do AWS Backup. Consulte também a [Página de preços](#).

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

Para criar uma conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções online.

Parte do procedimento de cadastro envolve uma chamada telefônica e a digitação de um código de verificação usando o teclado do telefone.

Anote o número da conta da AWS, pois você precisará dele na próxima tarefa.

Criar um usuário do IAM

Serviços em AWS, por exemplo, AWS Backup, exigem que você forneça credenciais quando acessá-las, para que o serviço possa determinar se você tem permissão para acessar seus recursos. O AWS recomenda que você não use o usuário raiz da conta da AWS 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. As credenciais do usuário administrador podem ser usadas, em vez das credenciais do usuário raiz da conta da AWS, para interagir com o AWS e executar tarefas, como criar um bucket, criar usuários e conceder permissões a eles. Para obter mais informações, consulte [Credenciais do usuário raiz da conta da AWS versus credenciais do IAM](#) no AWS Reference Architecture. Consulte também o [IAM User Guide](#).

Se você se cadastrou na AWS, mas não criou um usuário do IAM para você, crie um usando o console do IAM.

Para criar um usuário administrador para você mesmo e adicionar o usuário a um grupo de administradores (console)

1. Faça login no [Console do IAM](#) como o proprietário da conta escolhendo Usuário raiz e inserindo sua Conta da AWS, Endereço de e-mail. Na próxima página, insira sua senha.

Note

Recomendamos seguir as práticas recomendadas para utilizar o usuário do IAM **Administrator** a seguir e armazenar as credenciais do usuário root com segurança. Cadastre-se como o usuário root apenas para executar algumas [tarefas de gerenciamento de serviços e contas](#).

2. No painel de navegação, escolha Usuários e depois Adicionar usuário.
3. Em User name (Nome do usuário), digite **Administrator**.
4. Marque a caixa de seleção ao lado do acesso ao AWS Management Console. Então, selecione Custom password (Senha personalizada), e insira sua nova senha na caixa de texto.
5. (Opcional) Por padrão, a AWS exige que o novo usuário crie uma senha ao fazer login pela primeira vez. Você pode desmarcar a caixa de seleção próxima de User must create a new password at next sign-in (O usuário deve criar uma senha no próximo login) para permitir que o novo usuário redefina a senha depois de fazer login.
6. Selecione Next (Próximo): Permissions
7. Em Set permissions (Conceder permissões), escolha Add user to group (Adicionar usuário ao grupo).
8. Escolha Create group (Criar grupo).
9. Na caixa de diálogo Create group (Criar grupo), em Group name (Nome do grupo), digite **Administrators**.
10. Selecione Filter policies (Filtrar políticas) e, em seguida, selecione AWS managed - job function (Função de trabalho gerenciada da AWS) para filtrar o conteúdo da tabela.
11. Na lista de políticas, marque a caixa de seleção AdministratorAccess. A seguir escolha Criar grupo.

Note

Você deve ativar o acesso de usuário do IAM e da função para Billing (Faturamento) antes de usar as permissões de AdministratorAccess para acessar o console do AWS Billing and Cost Management. Para fazer isso, siga as instruções na [etapa 1 do tutorial sobre como delegar acesso ao console de faturamento](#).

12. Suporte a lista de grupos, selecione a caixa de seleção para seu novo grupo. Escolha Refresh (Atualizar) caso necessário, para ver o grupo na lista.
13. Selecione Next (Próximo): Tags.
14. (Opcional) Adicione metadados ao usuário anexando tags como pares de chave-valor. Para obter mais informações sobre como usar tags no IAM, consulte [Marcar entidades do IAM](#) no Manual do usuário do IAM.
15. Selecione Next (Próximo): Review (Revisar) Para ver uma lista de associações a grupos a serem adicionadas ao novo usuário. Quando você estiver pronto para continuar, selecione Criar usuário.

Você pode usar esse mesmo processo para criar mais grupos e usuários e conceder aos usuários acesso à sua conta da AWS recursos da AWS. Para saber como usar políticas para restringir as permissões de usuário a recursos específicos da AWS, consulte [Gerenciamento de acesso](#) e [Exemplos de políticas](#).

Para fazer login como novo usuário do IAM, saia da AWS Management Console. Em seguida, use o URL a seguir, onde `your_aws_account_id` é suas receitas AWS O número da conta da sem hífens (por exemplo, se suas receitas AWS O número da conta da 1234-5678-9012, suas receitas AWS O ID da conta da 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 a URL da página de cadastro contenha o ID da sua conta da AWS, crie um alias da conta. No painel do IAM, clique em **Criar Alias** da conta e insira um alias, como o nome da 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 da sua conta, abra o console do IAM e verifique em **AWSAccount Alias** (Alias da conta) No painel do.

Criar uma função do IAM

Você pode usar o console do IAM para criar uma função do IAM que conceda **AWS Backup** para acessar recursos suportados. Depois de criar a função do IAM, você pode criar e associar políticas à função.

Para criar uma função do IAM com o console

1. Faça login no **AWS Console** de Gerenciamento da e abra o [Console do IAM](#).
2. No console do IAM, escolha **Funções** do No painel de navegação e escolha **Crie uma função** do.
3. Selecione **AWS Funções de serviço** **doe**, depois, escolha **Select para AWS Backup**. Selecione **Continuar**.
4. No **Vincular políticas de permissões** **Página**, colar **AWS Backup Service Role Policy For Backup**, e **AWS Backup Service Role Policy For Restores**. Estes **AWS** **concessão** de políticas gerenciadas **AWS Backup** **Permissão** para fazer backup e restaurar todas as receitas com suporte **AWS** **recursos** da AWS. Para saber mais sobre políticas gerenciadas e ver exemplos, consulte [políticas gerenciadas pela](#).

Em seguida, escolha **Próximo: Tags**.

5. Selecione **Next (Próximo): Visão geral**.
6. Em **Role Name (Nome da função)**, digite um nome que descreva a finalidade da função. Os nomes de função devem ser exclusivos em sua conta da AWS. Como várias entidades podem fazer referência à função, não é possível editar o nome da função depois de sua criação.

Selecione **Create Role**.

7. Na página **Roles (Funções)**, escolha a função que você criou, para abrir a página de detalhes.

Conceitos básicos do AWS Backup

Este tutorial mostra as etapas gerais para fazer backup e restaurar qualquer recurso usando o AWS Backup. Se você quiser trabalhar com bancos de dados do Amazon RDS, siga este tutorial de 10 minutos: [Backup e restauração do Amazon Relational Database Service \(RDS\) usando AWS Backup](#). Se você quiser trabalhar com volumes do Amazon EBS, siga este tutorial de 10 minutos: [Tutorial: Backup e restauração do Amazon EBS usando o AWS Backup](#). Se você quiser trabalhar com sistemas de arquivos do Amazon FSx e funcionalidade entre regiões, entre contas, siga este blog: [Backups entre regiões e entre contas do Amazon FSx usando AWS Backup](#)

Tópicos

- [Prerequisites \(p. 17\)](#)
- [Opção 1: Criar um backup sob demanda \(p. 18\)](#)
- [Opção 2: Criar um backup agendado \(p. 19\)](#)
- [Opção 3: Criar backups automáticos do Amazon EFS \(p. 22\)](#)
- [Monitore seus trabalhos de backup e verifique se seus recursos estão protegidos \(p. 23\)](#)
- [Restaurar um backup \(p. 24\)](#)
- [Limpar os recursos \(p. 26\)](#)

Prerequisites

Antes de começar, verifique se você tem:

- Uma AWS; conta. Para obter mais informações, consulte [Configuração \(p. 14\)](#).
- Pelo menos um recurso suportado pelo AWS Backup.
- Você deve estar familiarizado com o AWS Serviços e recursos dos quais você está fazendo backup. Veja a lista de [compatível AWS Recursos e aplicativos de terceiros](#).

Quando novo AWS se tornarem disponíveis, habilite AWS Backup para usar esses serviços.

Para configurar o AWS Serviços a serem usados com o AWS Backup

1. Faça login no AWS Management Console e abra o AWS Backup console do em <https://console.aws.amazon.com/backup>.
2. No painel de navegação, selecione Settings.
3. Na página Optar pela adoção do serviço, escolha Configurar recursos.
4. No Configurar recursos Use as opções de alternância para habilitar ou desabilitar os serviços usados com o AWS Backup. Escolha Confirmar quando os serviços estiverem configurados. Verifique se o AWS o serviço que você está optando está disponível em seu AWS Região : Para obter mais informações sobre regiões compatíveis, consulte [Endpoints e cotas do serviço no AWS Referência geral](#).

Note

Se você configurar backups automáticos depois de habilitar o Amazon EFS para AWS Backup, seus backups automáticos continuarão mesmo se você desativar ou desativar o Amazon EFS para AWS Backup. Para obter mais informações, consulte [Opção 3: Criar backups automáticos do Amazon EFS \(p. 22\)](#). Para desabilitar backups automáticos, use o console do Amazon EFS ou a API.

- Certifique-se de que os recursos dos quais você está fazendo backup estão todos no mesmo AWS Região :

Para concluir este tutorial, você pode usar seu AWS Para fazer login no AWS Management Console. No entanto, AWS Identity and Access Management (IAM) recomenda que você não use o AWS Usuário raiz da conta da. Em vez disso, crie um perfil de administrador em sua conta e use essas credenciais para gerenciar os recursos dela. Para obter mais informações, consulte [Configuração \(p. 14\)](#).

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

Opção 1: Criar um backup sob demanda

No console do AWS Backup, a página Protected resources (Recursos protegidos) lista os recursos que foram submetidos a backup pelo AWS Backup pelo menos uma vez. Se estiver usando o AWS Backup Pela primeira vez, não há nenhum recurso, como volumes do Amazon EBS ou bancos de dados do Amazon RDS, listado 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 Protected resources (Recursos protegidos).

Como criar um backup sob demanda

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

Note

Para o Amazon FSx for Lustre, somente o tipo de implantação persistente é suportado.

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

Note

- Somente backups do Amazon EFS oferecem suporte à transição para armazenamento "frio". Todos os outros tipos de recurso são salvos no armazenamento "quente". O Expirar O valor é válido para todos os tipos de recursos.
 - Quando os backups expirarem e estiverem marcados para exclusão como parte de sua política de ciclo de vida, AWS Backup exclui os backups em um ponto escolhido aleatoriamente ao longo das 8 horas seguintes. Essa janela ajuda a garantir um desempenho consistente.
7. Escolha um cofre de backup existente. Ao escolher Create new backup vault (Criar novo cofre de backup) uma nova página será aberta para criar um cofre e você será redirecionado para a página Create on-demand backup (Criar backup sob demanda) ao concluir.

8. Em IAM role (Função do IAM), escolha Default role (Função padrão).

Note

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

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

Note

- Para recursos do Amazon EC2, AWS Backup copia automaticamente as tags de grupo e de recursos individuais existentes, além de todas as tags adicionadas a esse backup. Para obter mais informações, consulte [Cópia de tags em backups \(p. 48\)](#).
- Ao criar um plano de backup baseado em tags, se escolher função diferente da Função padrão, verifique se você tem as permissões necessárias para fazer backup de todos os recursos marcados. O 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 Create on-demand backup (Criar backup sob demanda). Dessa forma, você será redirecionado para a página Jobs (Trabalhos), onde verá uma lista de trabalhos.
11. Se o tipo de recurso for EC2, as Configurações avançadas de backup será exibida. Selecione VSS do Windows se sua instância do EC2 estiver executando o Microsoft Windows. Isso permite que você faça backups do Windows VSS consistentes com aplicativos.

Note

AWS Backup atualmente suporta backups consistentes com aplicativos de recursos em execução somente no Amazon EC2. Nem todos os tipos de instância ou aplicativos são suportados para backups do Windows VSS. Para obter mais informações, consulte [Criando backups do Windows VSS \(p. 47\)](#).

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

Próximas etapas

Para verificar o status e monitorar os detalhes da sua atividade de backup, prossiga para [Opção 2: Criar um backup agendado \(p. 19\)](#).

Opção 2: Criar um backup agendado

Na primeira etapa deste tutorial sobre o AWS Backup, você criará um plano de backup, atribuirá recursos a ele e criará um cofre de backup.

Antes de começar, verifique se você tem os pré-requisitos necessários. Para obter mais informações, consulte [Conceitos básicos do AWS Backup \(p. 17\)](#).

Tópicos

- [Etapa 1: Para criar um plano de backup modificando um plano existente \(p. 20\)](#)
- [Etapa 2: Atribuir recursos a um plano de backup \(p. 20\)](#)
- [Etapa 3: Criar um cofre de backup \(p. 21\)](#)
- [Próximas etapas \(p. 22\)](#)

Etapa 1: Para criar um plano de backup modificando um plano existente

Um plano de backup é uma expressão de política que define quando e como você quer fazer backup de seu AWS Recursos do, como tabelas do Amazon DynamoDB ou sistemas de arquivos do Amazon Elastic File System (Amazon EFS). Você pode atribuir recursos a planos de backup e, então, o AWS Backup, fará backup automaticamente e reterá backups para esses recursos de acordo com o plano de backup. Para obter mais informações, consulte [Gerenciando backups usando planos de backup \(p. 28\)](#).

Há duas maneiras de criar um novo plano de backup: É possível criar um do zero ou com base em um plano de backup existente. Este exemplo usa o console do AWS Backup 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 do em <https://console.aws.amazon.com/backup>.
2. No painel, escolha Gerenciar planos de backup. Em alternativa, usando o painel de navegação, selecione Planos de backup e escolha Criar plano de backup.
3. Selecione Iniciar com modelo. Escolha um plano da lista (por exemplo, Daily-Monthly-1yr-Retention) e insira um nome no Nome do plano de backup (Criar snapshot final?).

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, selecione a regra de backup desejada e escolha a opção Edite.
5. Analise e escolha os valores que você deseja aplicar à regra. Por exemplo, você pode estender o período de retenção do backup na regra Monthly (Mensal) para três anos, em vez de um ano. Se seu plano incluir backups do Amazon EFS, você pode configurar políticas de ciclo de vida que transferem automaticamente esses backups de armazenamento “quente” para armazenamento “frio” de acordo com a programação que você definiu.
6. Para o cofre de backup, escolha Padrão ou escolha Criar um novo cofre de backup para criar um novo cofre.
7. (Opcional) - escolha um AWS Região da lista em 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

Para aplicar planos de backup ao seu AWS Recursos do, escolha um plano de backup e atribua recursos a ele usando tags ou listando os IDs de recursos diretamente. Para obter mais informações sobre recursos, consulte [Atribuir recursos a um plano de backup \(p. 32\)](#).

Note

Se você estiver protegendo mais de 100 recursos em um plano, recomendamos que você use o gerenciamento baseado em tags.

Se você ainda não tiver o AWS Recursos que você deseja atribuir a um plano de backup, crie alguns recursos novos para usar neste exercício. Você pode criar vários recursos de vários ou de todos os [compatíveis AWS Recursos e aplicativos de terceiros](#).

Note

Para atribuir recursos por tags, você deve aplicar as tags aos seus recursos. Por exemplo, você pode marcar todos os recursos para este exercício com o par de chave/valor do `BackupPlan:MissionCritical`.

Como atribuir recursos a um plano de backup

1. No painel do console do AWS Backup, escolha Gerenciar planos de backup. No painel de navegação, selecione Planos de backup.
2. Escolha um plano da lista; por exemplo, `Daily-Monthly-1yr-Retention`.
3. Na página de resumo do plano, escolha Atribuir recursos.
4. No campo Nome de atribuição do recurso, escolha um nome para a atribuição de recurso.

Por exemplo, você pode nomear sua seleção de recursos como **ApplicationFoo**. Em seguida, você pode atribuir todos os AWS Recursos usados para esse aplicativo, o que pode ser uma combinação de volumes do Amazon EBS, sistemas de arquivos do Amazon EFS e tabelas do Amazon RDS.

5. Em IAM role (Função do IAM), escolha Default role (Função padrão).

Note

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

Se você escolher uma função diferente da função Função padrão, certifique-se de que sua função personalizada tenha as permissões necessárias para fazer backup de todos os recursos marcados. Para obter mais informações, consulte [Atribuir recursos a um plano de backup](#) (p. 32).

6. Na seção Assign resources (Atribuir recursos), certifique-se de que o comando Assign by (Atribuir por) exiba Tags. Insira uma chave e valor com os quais seus recursos estão marcados, por exemplo, **BackupPlan:MissionCritical**. Escolha Add assignment (Adicionar atribuição) para adicionar todos os recursos que estão marcados com o par de chave/valor escolhido.

Note

Ao criar um plano de backup baseado em tags, se escolher função diferente da Função padrão, verifique se você tem as permissões necessárias para fazer backup de todos os recursos marcados. O 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.

Todos os recursos com suporte na região selecionada que estão marcados com esse par de chave/valor são automaticamente atribuídos a esse plano de backup.

7. Quando um novo controle Atribuir por for exibido abaixo da primeira atribuição de recurso, altere o valor para **Resource ID**.
8. Escolha o tipo de recurso que você deseja adicionar à sua seleção, por exemplo, EBS. Coloque o cursor no campo ID do volume, e os recursos disponíveis para esse tipo serão exibidos.
9. Escolha um recurso na lista e clique em Adicionar atribuição.
10. Ao concluir a adição de recursos, escolha Assign resources (Atribuir recursos).

Depois, retorne para a página de resumo. Ela contém informações sobre o seu plano de backup, as regras de backup, as atribuições de recursos e todas as tags do 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 [Trabalhar com cofres de backup](#) (p. 35).

Como criar um cofre de backup

1. No console do AWS Backup, no painel de navegação, escolha Backup vaults (Cofres de backup).

Note

Se o painel de navegação não está visível no lado esquerdo, você pode abri-lo, escolhendo o ícone de menu no canto superior esquerdo do console do AWS Backup.

2. Escolha Create backup vault (Criar cofre de backup).
3. Insira um nome para o seu 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 poderia nomeá-lo como: **FinancialBackups**.
4. Selecione uma chave do AWS KMS. Você pode usar uma chave já existente ou selecionar o AWS BackupChave do KMS.

Note

A chave do AWS KMS especificada aqui se aplica apenas a backups de serviços que oferecem suporte à criptografia do AWS Backup. No momento, somente o Amazon Elastic File System (Amazon EFS) é compatível.

5. Opcionalmente, adicione tags que o ajudarão 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 Backup vaults (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 verificar o status e monitorar os detalhes da sua atividade de backup, prossiga para [Monitore seus trabalhos de backup e verifique se seus recursos estão protegidos](#) (p. 23).

Opção 3: Criar backups automáticos do Amazon EFS

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

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

1. Abra o console do Amazon EFS em <https://console.aws.amazon.com/efs>.

2. No **Sistemas de arquivos** Selecione o sistema de arquivos para o qual você deseja ativar backups automáticos.
3. Selecione **Edit** no painel **Configurações gerais**.
4. Para ativar os backups automáticos, selecione **Habilitar backups automáticos**.

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

Note

O cofre de backup automático do Amazon EFS `saws/efs/automatic-backup-vault` é reservado apenas para esses backups. Se você usá-lo como um destino para outros planos de backup, você receberá um erro de “privilégios insuficientes”.

AWS Backup cria uma função vinculada a serviços em seu nome na sua conta. Esta função tem as permissões necessárias para executar backups do Amazon EFS. Para obter informações detalhadas sobre funções vinculadas ao serviço, consulte [Funções vinculadas ao serviço para o AWS Backup](#) (p. 160).

Para obter instruções passo a passo sobre como ativar ou desativar backups automáticos usando o console do Amazon EFS, API ou CLI, consulte [Backups automáticos](#) no Amazon Elastic File System.

Monitore seus trabalhos de backup e verifique se seus recursos estão protegidos

AWS Backup permite que você visualize o status e outros detalhes da atividade de backup e restauração no AWS Serviços da que usar.

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

Tópicos

- [Exibir o status dos trabalhos de backup](#) (p. 23)
- [Exibir todos os backups em um cofre](#) (p. 24)
- [Exibir detalhes dos recursos protegidos](#) (p. 24)
- [Próximas etapas](#) (p. 24)

Exibir o status dos trabalhos de backup

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

Como visualizar o status dos trabalhos de backup

1. Abra o **AWS Backup console** do em <https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolha **Dashboard** (Painel).
3. Para visualizar o status de seus trabalhos de backup, escolha **Backup jobs details** (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.

Exibir 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 console do AWS Backup, no painel de navegação, escolha Backup vaults (Cofres de backup).
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 é geralmente Completed. Se por algum motivo o AWS Backup não pode excluir um backup de acordo com sua configuração de ciclo de vida, ele marca esse backup como Expired. Você será cobrado pelo armazenamento que Expired consome e devem excluí-los.

Exibir detalhes dos recursos protegidos

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

Como visualizar recursos protegidos

1. No console do AWS Backup, no painel de navegação, escolha Protected resources (Recursos protegidos).
2. Visualizar o AWS Recursos que estão sendo submetidos a backup. Escolha um recurso da lista para explorar seus backups associados a ele.

Próximas etapas

Depois de monitorar e verificar os backups de seu recurso, prossiga para [Restaurar um backup \(p. 24\)](#).

Restaurar um backup

Depois que um recurso foi submetido a backup pelo menos uma vez, ele é considerado protegido e está disponível para ser restaurado usando o 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 restaurar um backup usando a AWS CLI ou a API do AWS Backup, consulte [Restauração de um backup](#).

Como restaurar um recurso

1. Abrir o AWS Backup console do 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 [Restaurar um backup](#)

6. Para a Função de restauração, escolha Função padrão.

Note

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

7. Escolha Restore backup (Restaurar backup).

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

Note

Quando você executa uma restauração para restaurar itens específicos em uma instância do Amazon EFS, você pode restaurar esses itens em um sistema de arquivos novo ou existente. Se você restaurar os itens para um sistema de arquivos existente, o AWS Backup cria um novo diretório do 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, o 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 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.

Para 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, poderá restaurar arquivos e diretórios específicos usando a Restauração em nível de item. Para obter mais informações sobre a restauração de outros tipos de recursos, consulte [Restaurar um backup](#).

Note

Para restaurar uma instância do Amazon EFS, você deve “Permitir” `backup: startrestorejob`.

Para obter informações detalhadas sobre restauração, consulte [Restaurar um backup \(p. 61\)](#).

Próximas etapas

Após verificar os resultados da restauração, recomendamos excluir qualquer AWS Recursos que você não precisa manter, para não incorrer em cobranças desnecessárias. Para obter mais informações, consulte [Limpar os recursos \(p. 26\)](#).

Limpar os recursos

Depois de executar todas as tarefas no [Conceitos básicos do AWS Backup \(p. 17\)](#), você poderá limpar o que criou para evitar incorrer em cobranças desnecessárias.

Tópicos

- [Etapa 1: Excluir restauradoAWSrecursos \(p. 26\)](#)
- [Etapa 2: Excluir o plano de backup \(p. 26\)](#)
- [Etapa 3: Excluir os pontos de recuperação \(p. 26\)](#)
- [Etapa 4: Excluir o cofre de backup \(p. 27\)](#)

Etapa 1: Excluir restauradoAWSrecursos

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

Note

Isto se refere aos recursos restaurados, não aos pontos de recuperação armazenados em um cofre de backup.

Etapa 2: Excluir o plano de backup

Se você não deseja criar backups programados, deve excluir seus planos de backup. Você deve excluir todas as atribuições de recursos de um plano de backup antes de excluí-lo.

Siga estas etapas para excluir um plano de backup:

Como excluir um plano de backup

1. Abrir oAWS Backupconsole do em<https://console.aws.amazon.com/backup>.
2. No painel de navegação, selecione Backup plans (Planos de backup).
3. Na página Backup plans (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 Delete (Excluir).
5. Para excluir o plano de backup, escolha Delete (Excluir) no canto superior direito da página.
6. Na página de confirmação, insira o nome do plano e escolha Delete plan (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 console do AWS Backup, no painel de navegação, escolha Backup vaults (Cofres de backup).
2. Na página Backup vaults (Cofres de backup), escolha o cofre no qual você armazenou os backups.
3. Verifique o ponto de recuperação e escolhaExcluir.
4. Se você estiver excluindo mais de um ponto de recuperação, execute estas etapas:

- a. Revise a lista de pontos de recuperação que você está excluindo.
- b. Se você quiser editar a lista, selecione **Modify** seleção.
- c. Se sua lista contiver um backup contínuo, escolha se deseja manter ou excluir seus dados de backup contínuo.
- d. Para excluir todos os pontos de recuperação listados, digite **delete**, depois, escolha **Excluir** pontos de recuperação.

Mantenha a guia do navegador aberta até ver o banner de sucesso verde na parte superior da página.

Fechar prematuramente esta guia encerrará o processo de exclusão e poderá deixar para trás alguns dos pontos de recuperação que você deseja excluir.

Etapa 4: Excluir o cofre de backup

Não é possível excluir o cofre de backup padrão no AWS Backup. No entanto, se você criou um cofre de backup diferente, esvazie-o para excluir os backups. Depois, selecione o cofre de backup e escolha **Delete** (**Excluir**).

Gerenciando backups usando planos de backup

Dentro do AWS Backup, um plano de backup é uma expressão de política que define quando e como você quer fazer backup dos recursos do, 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 o AWS Backup automaticamente fará e reterá backups desses recursos de acordo com o plano de backup. Você poderá criar vários planos de backup se tiver cargas de trabalho com diferentes requisitos de backup.

As seções a seguir fornecem os conceitos básicos de gerenciamento de sua estratégia de backup no AWS Backup.

Tópicos

- [Como criar um plano de backup \(p. 28\)](#)
- [Atribuir recursos a um plano de backup \(p. 32\)](#)
- [Excluir um plano de backup \(p. 33\)](#)
- [Atualizar um plano de backup \(p. 33\)](#)

Como criar um plano de backup

Quando você cria um plano de backup, ele é adicionado ao conjunto de planos em sua conta. Você também pode usar o modelo do AWS CloudFormation para criar um plano de backup. Para obter mais informações, consulte [AWS Backup Referência do tipo de recurso](#) no AWS CloudFormation Guia do usuário.

Tópicos

- [Criando planos de backup usando o AWS Management Console \(p. 28\)](#)
- [Opções e configuração do plano de backup \(p. 29\)](#)

Criando planos de backup usando o AWS Management Console

O AWS Backup fornece duas maneiras para começar a usar o console do AWS Backup:

- **Inicie com um plano existente** — Você pode criar um plano de backup com base nas configurações de um plano existente. Esteja ciente de que os planos de backup criados pelo AWS Backup baseiam-se nas melhores práticas e nas configurações comuns de política de backup. Ao optar por iniciar com um plano existente, as configurações desse plano de backup são preenchidas automaticamente no seu novo plano de backup. Você pode, então, alterar qualquer uma dessas configurações de acordo com as exigências do seu backup.

Para obter instruções passo a passo, consulte [Etapa 1: Para criar um plano de backup modificando um plano existente \(p. 20\)](#) na seção Conceitos básicos.

- **Criar um plano do zero** — Você pode criar um plano de backup especificando cada um dos detalhes da configuração de backup, conforme descrito na próxima seção. Você pode escolher entre as configurações padrão recomendadas.

Note

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

Opções e configuração do plano de backup

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

Nome do plano de backup

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

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

Regras de backup

Os planos de backup contêm uma ou mais regras de backup. Cada regra de backup consiste nos elementos a seguir.

Note

Se você tiver um plano de backup com várias regras se o período de tempo das duas regras se sobrepor, AWS Backup otimiza o backup e faz um backup para a regra com maior tempo de retenção. A otimização leva em conta a janela de início completo, não apenas quando o backup diário é feito.

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.

Backup frequency (Frequência de backup)

A frequência de backup determina a frequência com que AWS Backup cria um backup de snapshot. Usando o console, você pode escolher uma frequência de cada hora, 12 horas, diariamente, semanalmente ou mensalmente. Você também pode criar uma expressão cron que cria backups de instantâneos com a frequência de hora em hora. Usar o AWS Backup CLI, você pode agendar backups de snapshot com a frequência de hora em hora.

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

Você também pode conferir o [Ativar backups contínuos para recursos suportados](#) Para criar uma regra de backup contínuo habilitada para restauração point-in-time (PITR). Ao contrário dos backups de snapshots, os backups contínuos permitem que você execute a restauração point-in-time. Para saber mais sobre backups contínuos, consulte [Recuperação point-in-time](#).

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. Se não tiver certeza de qual janela de backup usar, você poderá optar por usar a janela de backup padrão que o AWS Backup recomenda. A janela de backup padrão é definida para iniciar às 5h UTC (Tempo Universal Coordenado) e dura 8 horas.

Note

É possível personalizar a frequência de backups e o horário de início da janela de backup usando uma expressão cron. Para obter mais informações sobre expressões cron, consulte [Programar expressões para regras](#) no Amazon CloudWatch Events Guide. Recomendamos testar sua expressão cron usando um dos muitos geradores cron disponíveis e ferramentas de teste.

Note

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

Note

AWS Backup cancela qualquer trabalho de backup agendado 4 horas antes da janela de manutenção ou janela de backup automatizado de qualquer AWS recurso de banco de dados. Isso é para garantir a integridade dos dados de seus bancos de dados. AWS inclui, mas não estão limitados a, instâncias do Amazon RDS, clusters do Aurora e tabelas do Amazon DynamoDB. Para evitar falhas nas tarefas de backup, execute um dos seguintes procedimentos:

- Configure seus planos de backup para serem executados pelo menos 4 horas antes (ou imediatamente após) das janelas de backup desses serviços, ou
- Usar o AWS Backup planos e regras para executar backups instantâneos e contínuos. Consulte [Recuperação point-in-time](#) para ver as instruções. AWS Backup suporta somente esse recurso para o Amazon RDS (não incluindo o Amazon Aurora). AWS Backup irá programar de forma inteligente ambas as janelas de backup para evitar um possível conflito.

Sobrepôr regras de backup

Ocasionalmente, um plano de backup pode conter várias regras sobrepostas. Quando as janelas de início de diferentes regras 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. Backup por hora, com uma janela de início de 1 hora, e mantenha por 1 dia.
2. Faça backup a cada 12 horas, com uma janela de início de 8 horas, e mantenha por 1 semana.

Após 24 horas, a segunda regra cria dois backups (porque tem o período de retenção mais longo). A primeira regra cria oito backups (porque a janela de início de 8 horas da segunda regra impediu a execução de mais backups por hora). Especificamente:

Durante esta Janela Inicial	Esta regra cria 1 backup
Meia-noite às 8h	12 horas
8 a 9	Por hora
9 a 10	Por hora
10 para 11	Por hora
11 ao meio-dia	Por hora
Meio-dia às 20h	12 horas
8 a 9	Por hora
9 a 10	Por hora

Durante esta Janela Inicial	Esta regra cria 1 backup
10 para 11	Por hora
11 à meia-noite	Por hora

Lifecycle

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.

Se você quiser que seus backups sejam incrementais, você deve ter pelo menos um backup quente. Como cada backup em armazenamento frio é um backup completo, AWS BackupA recomenda que você defina as configurações do ciclo de vida para não mover o backup para o armazenamento frio até depois de pelo menos 8 dias.

Se você definir seu ciclo de vida para fazer backup em armazenamento frio após 1 dia, cada um desses backups será um backup completo. Isso pode ser menos econômico do que uma transferência menos regular para armazenamento frio.

Os backups transferidos para o armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, no console, a configuração de "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao armazenamento 'frio'". Não é possível alterar a configuração do "número de dias para transição para armazenamento frio" depois que a transição para "frio" foi habilitada.

Note

- Atualmente, apenas os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio". A expressão de armazenamento frio é ignorada para os backups do Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Aurora, Amazon DynamoDB e AWS Storage Gateway.
- Quando os backups atingem o fim do ciclo de vida e estiverem 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 de 8 horas ajuda a garantir um desempenho consistente para exclusão.

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 do AWS Key Management Service (AWS KMS) usada para criptografar backups no cofre e para controlar o acesso aos backups no cofre. 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 obter instruções passo a passo para a criação de um cofre de backup, consulte [Etapa 3: Criar um cofre de backup \(p. 21\)](#).

Copiar em regiões

Como parte do plano de backup, você pode, opcionalmente, criar uma cópia de backup em outra AWS Região : Para obter mais informações sobre cópias de backup, consulte <https://docs.aws.amazon.com/aws-backup/latest/devguide/recov-point-create-a-copy.html#create-cross-account-backup>.

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) Função do IAM

A função do IAM que AWS Backup usa ao criar a cópia. A função também deve ter AWS Backup listada como uma entidade confiável, que permite AWS Backup para assumir a função. Quando escolher Padrão e a função padrão do AWS Backup não estiver presente em 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.

Marcas adicionadas aos pontos de recuperação

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

Marcas 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

Permite backups consistentes com aplicativos para aplicativos de terceiros que estão sendo executados em instâncias do Amazon EC2. Atualmente, AWS Backup suporta cópias de segurança do Windows VSS. AWS Backup exclui tipos específicos de instância do Amazon EC2 dos backups do Windows VSS. Para obter mais informações, consulte [Criando backups do Windows VSS \(p. 47\)](#).

Atribuir recursos a um plano de backup

Quando você atribui um recurso a um plano de backup, esse recurso é automaticamente submetido a backup de acordo com o plano de backup. Os backups desse recurso são gerenciados de acordo com o plano de backup. Você pode atribuir recursos usando tags ou IDs de recurso.

Note

Se você estiver protegendo mais de 100 recursos em um plano, recomendamos que você use o gerenciamento baseado em tags.

Usar tags para atribuir recursos é uma maneira simples e dimensionável de fazer backup de vários recursos. Qualquer recurso com as tags que você especifica na atribuição de recursos é atribuído ao plano de backup. Por exemplo, se você atribuir recursos com os valores de tag `July` e `August`, você atribuiu todos os seus recursos marcados com `July` ou `August`. Observe que as tags fazem distinção entre maiúsculas e minúsculas.

Por exemplo, é possível definir um plano de backup que atenda aos seus requisitos de backup para dados de missão crítica e criar uma atribuição de recursos com a chave de `tagClassificationValor` da `tagMissionCritical`. Assim, qualquer recurso com essa tag será automaticamente atribuído ao seu plano de backup de missão crítica.

Note

Ao criar um plano de backup baseado em tags, se você escolher uma função diferente da função padrão, verifique se ele tem as permissões necessárias para fazer backup de todos os recursos marcados. O 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.

Para obter instruções passo a passo para a atribuição de recursos a um plano de backup, consulte [Etapa 2: Atribuir recursos a um plano de backup](#) (p. 20) na seção Conceitos básicos.

Excluir um plano de backup

Você pode 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 atuais e anteriores (se houver) ainda existem, mas elas não estão mais listadas no console em Backup plans (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.

Como excluir um plano de backup usando o console do AWS Backup

1. Faça login no AWS Management Console, e abra o AWS Backup console do em <https://console.aws.amazon.com/backup>.
2. No painel de navegação no lado esquerdo, selecione Backup plans (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 Delete.

Atualizar um plano de backup

Depois de criar um plano de backup, você pode editar o plano — por exemplo, é possível adicionar tags ou 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.

Como editar um plano de backup usando o console do AWS Backup

1. Abrir o AWS Backup console do em <https://console.aws.amazon.com/backup>.
2. No painel de navegação, selecione Backup plans (Planos de backup).
3. Escolha uma regra de backup e escolha Edit (Editar).

4. Na regra de backup, faça as alterações nas configurações desejadas e selecione Save (Salvar).

Trabalhar com cofres de backup

Dentro AWS Backup, um Cofre de backup é um contêiner que armazena e organiza seus backups. Você pode usar cofres de backup para definir a chave de criptografia do AWS Key Management Service (AWS KMS) usada para criptografar backups no cofre e para controlar o acesso aos backups no cofre. Caso você precise de diferentes chaves de criptografia ou políticas de acesso para diferentes grupos de backups, é possível criar vários cofres de backup. Caso contrário, você pode ter todos os seus backups organizados no cofre de backup padrão.

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

Tópicos

- [Como criar um cofre de backup \(p. 35\)](#)
- [Definindo políticas de acesso em cofres de backup e pontos de recuperação \(p. 36\)](#)
- [Excluir um cofre de backup \(p. 39\)](#)

Como criar um cofre de backup

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

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

No entanto, se você usar `AWS Backup` por meio do `AWS CLI`, `AWSSDK` ou `AWS CloudFormation`, um cofre padrão não é criado. Você deve criar seu próprio cofre.

Uma `AWS P`ode criar até 100 cofres de backup por `AWS Região` :

Para obter instruções passo a passo para a criação de um cofre de backup, consulte [Etapa 3: Criar um cofre de backup \(p. 21\)](#) na seção Conceitos básicos.

Ao criar um cofre de backup, você pode definir os elementos a seguir.

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, hífen ou sublinhados.

Chave de criptografia do KMS

O `AWS KMS` A chave de criptografia protege seus backups neste cofre de backup. Por padrão, o `AWS Backup` cria uma chave KMS com o alias `aws/backup` para você. Você pode escolher essa chave ou qualquer outra chave na sua conta.

Você pode criar uma nova chave mestra de criptografia seguindo a seção [Criação de chaves](#) no `AWS Key Management Service` Guia do desenvolvedor.

Depois de criar um cofre de backup e definir a propriedade `AWS KMS` Chave de criptografia do, você não pode mais editar a chave para esse cofre de backup.

A chave de criptografia especificada em um cofre do `AWS Backup` se aplica aos backups de determinados tipos de recursos. Para obter mais informações sobre a criptografia de backup, consulte [Criptografia para](#)

[backups noAWS \(p. 94\)](#) na seção Segurança. Os backups de todos os outros tipos de recurso são feitos com a chave usada para criptografar o recurso de origem.

Tag do cofre de backup

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

Definindo políticas de acesso em cofres de backup e pontos de recuperação

comAWS BackupVocê 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 o uso das políticas do para conceder ou restringir o acesso a recursos, consulte [Políticas baseadas em identidade e em recursos](#) no IAM User Guide. Você também pode controlar o acesso usando tags.

Você pode usar os exemplos de políticas a seguir como um guia para limitar o acesso a recursos quando estiver trabalhando com cofres do AWS Backup.

Important

Ao contrário de outras políticas baseadas em IAM, AWS Backup políticas de acesso não suportam um caractere curinga no ActionChave do.

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 do recurso \(p. 100\)](#) para ARNs de pontos de recuperação específicos dos recursos.

Note

Independentemente do AWS Backup política de acesso do vault, AWS Backup prejeitará qualquer 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 \(p. 36\)](#)
- [Negar acesso a um cofre de backup \(p. 37\)](#)
- [Negar acesso a excluir pontos de recuperação em um cofre de backup \(p. 37\)](#)

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 Amazon EBS em um cofre de backup.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement ID",
```

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

Note

Esta política de acesso controla somente o acesso de usuários às APIs do AWS Backup. Alguns tipos de backup, como snapshots do Amazon Elastic Block Store (Amazon EBS) e Amazon Relational Database Service (Amazon RDS), também podem ser acessados 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 aos backups.

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": [
    {
      "Sid": "statement ID",
      "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 a 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 noAWS Management Console, e abra oAWS Backupconsole do em<https://console.aws.amazon.com/backup>.
2. No painel de navegação no lado esquerdo, selecione Backup vaults (Cofres de backup).
3. Selecione um cofre de backup na lista.
4. Na seção de Access policy (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. Substituir *ID da instrução*, eaws:userId(*Função/MyRole*) com valores para seu ambiente.

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

Para permitir identidades do IAM de lista usando seu ARN, use oaws:PrincipalArnchave de condição global no exemplo a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement ID",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "backup:DeleteRecoveryPoint",
      "Resource": "*",
      "Condition": {
        "StringNotLike": {
          "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 IAM User Guide.

Se você quiser limitar isso a tipos de recursos específicos, em vez de "Resource": "*", você pode 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.

Excluir um cofre de backup

Para se proteger contra exclusão em massa acidental ou maliciosa, você só pode excluir um cofre de backup no AWS Backup depois de eliminar (ou os ciclos de vida da política de cópia de segurança) todos os pontos de recuperação no cofre de cópia de segurança. Para excluir todos os pontos de recuperação manualmente, consulte essa seção em [Limpar os recursos](#).

Como excluir um cofre de backup usando o console do AWS Backup

1. Faça login no AWS Management Console, e abra o AWS Backup console do em <https://console.aws.amazon.com/backup>.
2. No painel de navegação, selecione Backup vaults (Cofres de backup).
3. Escolha o cofre de backup que você deseja excluir.
4. Escolha e exclua todos os backups associados ao cofre de backup.
5. Exclua o cofre de backup escolhendo Excluir (no canto superior direito).

Note

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.

Trabalhar com backups

Uma cópia de segurança 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 momento determinado. Ponto de recuperação é um termo que se refere geralmente aos diferentes backups no AWS, 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 empresariais. Por exemplo, você pode salvar um conjunto de recursos que contém informações financeiras para o ano fiscal de 2020. Quando você precisa recuperar um recurso, você pode usar o console do AWS Backup ou a AWS Command Line Interface (AWS CLI) para localizar e recuperar o recurso de que você precisa.

Cada ponto de recuperação tem um ID exclusivo. A tabela a seguir contém o AWS Tipos de recursos do que AWS Backup oferece suporte e exemplos de seu ID de ponto de recuperação correspondente.

Tipo de recurso	Nome do backup	Exemplo de ID do ponto de recuperação
Sistema de arquivos do Amazon FSx	Backup do Amazon FSx	backup/ backup-0ecdf967356c809c7
Instância do Amazon Elastic Compute Cloud (Amazon EC2)	Backup do Amazon EC2	image/ ami-0ecdf967356c809c7
Volume do Amazon EBS	Snapshot do Amazon EBS	snapshot/ snap-05f426fd8kdjb4224
Banco de dados do Amazon RDS	Snapshot do Amazon RDS	awsbackup:job- be59cf2a-2343-4402- bd8b-226993d23453
Cluster de banco de dados do Amazon	Clusters Aurora	awsbackup:job- be59cf2a-2343-4402- bd8b-226993d23453
Sistema de arquivos do Amazon EFS	Backup do Amazon EFS	d99699e7-e183-477e-bfcd- ccb1c6e5455e
DynamoDB tabela	Backup do DynamoDB	table/MyDynamoDBTable/ backup/01547087347000- c8b6kdk3
Volume do AWS Storage Gateway	Snapshot do Amazon EBS*	snapshot/ snap-0d40e49137e31d9e0

*Quando você faz backup de um AWS Storage Gateway, um snapshot do Amazon EBS será criado. Esse snapshot pode ser restaurado como um volume do Amazon EBS ou como um AWS Storage Gateway volume do.

Important

Para evitar cobranças adicionais, configure sua política de retenção com uma duração de armazenamento quente de pelo menos uma semana.

AWS Backup calcula seu ciclo de vida a partir do início do trabalho de backup, não da conclusão. Por exemplo, suponha que você faça backups diários e os mantenha por um dia. Suponha ainda que seus recursos protegidos sejam tão grandes que leva o dia inteiro para concluir o backup. AWS Backup implementará seu período de renúncia de um dia e removerá seu backup do armazenamento quente quando o trabalho de backup for concluído. No dia seguinte, AWS Backup não pode criar um backup incremental porque não há backup no armazenamento quente. 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. Peça orientação ao seu gerente técnico de conta ou arquiteto de soluções sobre seu caso de uso.

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

Tópicos

- [Criar um backup \(p. 41\)](#)
- [Copiar um backup \(p. 49\)](#)
- [Visualizar uma lista de backups \(p. 59\)](#)
- [Editar um backup \(p. 60\)](#)
- [Restaurar um backup \(p. 61\)](#)

Criar um backup

No AWS Backup, você pode criar backups automaticamente usando planos de backup ou iniciando um backup sob demanda manualmente.

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 [Gerenciando backups usando planos de backup \(p. 28\)](#).

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. Cada trabalho de backup tem uma ID exclusiva — por exemplo, D48D8717-0C9D-72DF-1F56-14E703BF2345.

Você pode visualizar o status de um trabalho de backup na página Jobs (Trabalhos) do console do AWS Backup. Os status dos trabalhos de backup incluem: criado, pendente, em execução, cancelando, cancelado, concluído, falhou e expirado.

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

Por exemplo, se o backup do dia 1 (completo) tiver sido excluído devido a uma política de ciclo de vida de 3 dias, você ainda poderá executar uma restauração completa com os backups dos dias 2 e 3. AWS Backup mantém os dados de referência necessários a partir do dia 1 para permitir isso.

Para obter mais informações sobre como criar planos de backup, consulte [Como criar um plano de backup \(p. 28\)](#).

Tópicos

- [Criar um backup sob demanda \(p. 42\)](#)
- [Restaurando para um tempo especificado usando recuperação point-in-time \(p. 43\)](#)

- [Criando backups do Windows VSS \(p. 47\)](#)
- [Como criar backups consistentes com falhas e multivolume do Amazon EBS \(p. 48\)](#)
- [Copiar tags em backups \(p. 48\)](#)
- [Interromper um trabalho de backup \(p. 49\)](#)

Criar um backup sob demanda

No console do AWS Backup, a página Protected resources (Recursos protegidos) lista os recursos que foram submetidos a backup pelo AWS Backup pelo menos uma vez. Se estiver usando o AWS Backup pela primeira vez, não há nenhum recurso (como volumes do Amazon EBS ou bancos de dados do Amazon RDS) listado 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.

Como criar um backup sob demanda

1. Abrir o AWS Backup console do <https://console.aws.amazon.com/backup>.
2. No painel, escolha Create an on-demand backup (Criar um backup sob demanda). Ou, no painel de navegação, escolha Protected resources (Recursos protegidos) e Create an on-demand backup (Criar backup sob demanda).
3. No Criar backup sob demanda, selecione o tipo de recurso do qual você deseja fazer backup; por exemplo, escolha DynamoDB para tabelas do Amazon DynamoDB.
4. Escolha o nome ou ID do recurso que você deseja proteger; por exemplo, VideoMetadataTable.
5. Certifique-se de que a opção Create backup now (Criar backup agora) esteja selecionada. Isso inicia um backup imediatamente e permite que você consulte antes o recurso salvo na página Protected resources (Recursos protegidos).
6. Se você estiver usando o Amazon EBS, DynamoDB, Amazon RDS, Amazon Aurora ou AWS Storage Gateway, o valor está marcado N/A porque esses tipos de recursos não podem ser salvos no armazenamento frio.

Se você estiver usando o Amazon EFS, escolha o valor desejado para especificar quando esse backup será transferido para o armazenamento "frio".

7. Escolha um valor de Expire (Vencimento).

Note

Quando os backups expirarem e estiverem marcados para exclusão como parte de sua política de ciclo de vida, o AWS Backup exclui os backups em um ponto escolhido aleatoriamente ao longo das 8 horas seguintes. Essa janela ajuda a garantir um desempenho consistente.

8. Escolha um Backup vault (Cofre de backup) existente ou crie um. Ao escolher Create new Backup vault (Criar novo cofre de backup), uma nova página será aberta para criar um cofre e você será redirecionado para a página Create on-demand backup (Criar backup sob demanda) quando terminar.
9. Em Função do IAM, escolha Função padrão ou uma função de sua escolha.

Note

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

10. Para 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, o AWS Backup copia automaticamente as tags de grupo e de recursos individuais existentes, além de todas as tags adicionadas nesta etapa.

11. Se o recurso que você deseja fazer backup estiver executando uma instância do Amazon EC2, escolha VSS do Windows no Configurações avançadas da seção. Isso permite que você faça backups do Windows VSS consistentes com aplicativos.

Note

AWS Backup faz backups do EC2 com “sem reinicialização” como comportamento padrão. AWS Backup atualmente suporta recursos em execução no Amazon EC2, e determinados tipos de instância não são compatíveis. Para obter mais informações, consulte [Criando backups do Windows VSS \(p. 47\)](#).

12. Escolha Create on-demand backup (Criar backup sob demanda). Isso leva você ao Trabalho do, onde você pode ver uma lista de trabalhos.
13. Selecione o ID do trabalho de backup. Para obter o recurso que você escolheu fazer backup. Na página de detalhes do trabalho, pause o mouse sobre Status para visualizar os detalhes do status do trabalho.

Restaurando para um tempo especificado usando recuperação point-in-time

AWS Backup suporta backups contínuos e recuperação point-in-time (PITR), além de backups de snapshot. Com backups contínuos, você pode restaurar seu AWS Backup-suportado, rebobinando-o de volta para um tempo específico que você escolher, dentro de 1 segundo de precisão (retrocedendo um máximo de 35 dias). Compare isso com backups de snapshot, que você só pode fazer com a frequência de cada hora. Você também pode armazenar backups de snapshot por um máximo de 100 anos. Como os backups contínuos e instantâneos oferecem vantagens diferentes, recomendamos que você proteja seus recursos com regras de backup contínuo e instantâneo.

O backup contínuo funciona primeiro criando um backup completo do seu recurso e, em seguida, constantemente fazendo backup dos logs de transação do seu recurso. A restauração do PITR funciona acessando seu backup completo e reproduzindo o log de transações para o horário que você informar AWS Backup para recuperar.

Você pode ativar backups contínuos ao criar um plano de backup no AWS Backup ou a AWS Backup ou a API.

Para habilitar backups contínuos usando o console

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

Serviços e aplicativos suportados para recuperação point-in-time

AWS Backup oferece suporte a backups contínuos e a recuperação point-in-time dos serviços e aplicativos a seguir. Esta seção descreve as vantagens, limitações e práticas recomendadas específicas de recursos para usar o PITR no AWS Backup.

Amazon RDS

O Amazon RDS chama seus backups contínuos de “backups automatizados”. AWS Backup chama backups contínuos do Amazon RDS de “backups contínuos”.

Se você usar AWS Backup para snapshots do Amazon RDS e backups contínuos, AWS Backup programará de forma inteligente suas janelas de backup, juntamente com a janela de manutenção do Amazon RDS, para evitar conflitos. Você não precisa mais agendar manualmente uma janela de backup horas antes da outra.

Note

AWS Backup atualmente não é compatível com backups contínuos do Amazon Aurora. AWS Backup suporta snapshots do Aurora.

Você não pode controlar a janela de backup automatizado do Amazon RDS. Isto é porque AWS Backup agenda de forma inteligente para você.

Você pode executar uma recuperação point-in-time usando AWS Backup ou Amazon RDS. Para o AWS Backup, instruções do console, consulte [Restauração de um banco de dados Amazon RDS](#). Para obter instruções do Amazon RDS, consulte [Restauração de uma instância de banco de dados para um horário especificado](#) no Guia do usuário do Amazon RDS.

Lembre-se do seguinte ao executar uma recuperação point-in-time:

- Restaurar atividade recente— talvez você não consiga restaurar os 5 minutos mais recentes de atividade devido à forma como o Amazon RDS lida com seus logs de transação.
- Criação de cópias de backups contínuos do Amazon RDS— Você não pode criar cópias de backups contínuos do Amazon RDS porque o Amazon RDS não permite copiar logs de transação.

Para obter informações gerais sobre como trabalhar com o Amazon RDS, consulte o [Guia do usuário do Amazon RDS](#).

Gerenciando configurações de backup contínuo

Depois de aplicar um AWS Backup regra de backup contínuo para uma instância do Amazon RDS, você não pode criar ou modificar configurações de backup contínuo para essa instância no Amazon RDS. Esta limitação existe para evitar conflitos.

Para visualizar seu backup contínuo no Amazon RDS, abra a página de detalhes da instância no [Console do Amazon RDS](#), escolha Manutenção e backup, e localize o Backup automatizado campo.

Para fazer a transição do controle de backup contínuo dessa instância do Amazon RDS de volta para o Amazon RDS, você pode usar o AWS Backup console, o AWS CLI ou API.

Para fazer a transição do controle contínuo de backup para o Amazon RDS usando o AWS Backup console

1. Abrir o AWS Backup console do <https://console.aws.amazon.com/backup>.
2. No painel de navegação, selecione Backup plans (Planos de backup).
3. Exclua todos os planos de backup do Amazon RDS com backup contínuo protegendo esse recurso.
4. Escolha Cofres de backup. Exclua o ponto de recuperação de backup contínuo do seu cofre de backup. Ou aguarde que o período de retenção decorra, causando AWS Backup Para excluir automaticamente o ponto de recuperação.

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

Para fazer a transição do controle contínuo de backup para o Amazon RDS usando o AWS Backup API ou CLI

- Chame o `DisassociateRecoveryPoint` Operação da API.

Para saber mais, consulte [DisassociateCoveyPoint](#).

Permissões 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 plano de backup. Para restaurar backups contínuos do Amazon RDS, você deve adicionar a permissão `rds:RestoreDBInstanceToPointInTime` à função do IAM enviada para o trabalho de restauração. Você pode usar o `AWS Backup default service role` para executar backups e restaurações.
- Para descrever o intervalo de tempo disponível para recuperação point-in-time, use `AWS Backup Call rds:DescribeDBInstanceAutomatedBackups` API. No `AWS Backup Console`, você deve ter a permissão `rds:DescribeDBInstanceAutomatedBackups` da API no seu `AWS Identity and Access Management` política gerenciada (IAM). Você pode usar o `AWS Backup Full Access` ou `AWS Backup Operator Access` Políticas gerenciadas do. Ambas as políticas têm todas as permissões necessárias. Para obter mais informações, consulte [Políticas gerenciadas do](#).

Trabalhar com backups contínuos

Encontrar um backup contínuo

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

Para localizar um backup contínuo usando o comando AWS Backup console

1. Abrir o AWS Backup console do <https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolha **Cofres de backup** e escolha seu cofre de backup na lista.
3. No **Backups** do, na seção **Tipo de backup** coluna, classificar para **Continuous** Pontos de recuperação. Você também pode classificar por **ID do ponto de recuperação** para o prefixo **Continuous**.

Restaurar um backup contínuo

Para restaurar um backup contínuo usando o comando AWS Backup console

- Durante o processo de restauração do PITR, o AWS Backup exibe um **Tempo de restauração** seção. Nesta seção, proceda de uma das seguintes maneiras:
 - Opte por restaurar para a pasta **Último horário restaurável**.
 - Selecione **Especificar data e hora** para inserir sua própria data e hora dentro do período de retenção.

Para restaurar um backup contínuo usando o comando AWS Backup API

- Chame o `StartRestoreJob` Operação da API com o `RestoreTime`, como no exemplo a seguir.

```
"RestoreTime": "2011-09-07T23:45:00Z"
```

Você deve expressar `RestoreTime` em Tempo Universal Coordenado (UTC). Para obter mais informações, consulte [RestoreTime](#).

Interromper backup contínuo

Se desejar interromper backups contínuos, você deve excluir a regra de backup contínuo do plano de backup. Se, em vez disso, você excluir apenas um ponto de recuperação de backup contínuo do cofre de

backup, o plano de backup continuará a executar a regra de backup contínuo, criando um novo ponto de recuperação.

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

Fazendo cópias de backups contínuos

Se uma regra de backup contínuo também especificar uma cópia entre contas ou entre regiões, o AWS Backup tira um instantâneo do backup contínuo, copia esse instantâneo para o cofre de destino e, em seguida, exclui o instantâneo de origem. Para saber mais sobre como copiar seus pontos de recuperação entre contas e regiões, consulte [Copiar um backup](#).

O AWS Backup não oferece suporte a cópias sob demanda de backups contínuos. O AWS Backup não oferece suporte a cópias de backups contínuos do Amazon RDS porque o Amazon RDS não permite cópias de seus logs de transação.

Alterar o período de retenção

Você pode usar o AWS Backup para aumentar ou diminuir o período de retenção para a 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 seu período de retenção, o efeito é imediato. Se você diminuir o período de retenção, o AWS Backup guardará até que passe tempo suficiente antes de aplicar a alteração para proteger contra perda de dados. Por exemplo, se você diminuir o período de retenção de 35 dias para 20 dias, o 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.

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

Quando criar um plano de cópia de segurança com uma regra de cópia de segurança contínua e, em seguida, remover essa regra, o AWS Backup lembra o período de retenção da regra agora excluída. Ele excluirá o backup contínuo do seu cofre de backup quando o período de retenção terminar.

Sobreposição de backups contínuos no mesmo recurso

Em geral, você deve proteger cada recurso com não mais do que uma regra de backup contínuo. Isso ocorre porque os backups contínuos adicionais são redundantes. No entanto, à medida que você aumenta sua propriedade de backup, é possível que vários planos de backup, regras e cofres se sobreponham em um único recurso. O AWS Backup manipula essas sobreposições da seguinte forma.

Se você incluir o mesmo recurso em mais de um plano de backup com uma regra de backup contínuo, o AWS Backup criará somente um backup contínuo para o primeiro plano de backup que ele avaliar. Ele criará backups de instantâneos 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, o AWS Backup cria apenas um backup contínuo para a regra com o período de retenção mais longo. Desrespeita todas as outras regras.
- Se suas regras apontarem para cofres de backup diferentes, o AWS Backup rejeita o plano como não válido.

Considerações sobre recuperação point-in-time

Lembre-se das seguintes considerações sobre a recuperação point-in-time:

- **Fallback automático para snapshots**— Se o AWS Backup não conseguir executar um backup contínuo, ele tenta executar um `snapshotBackup` em vez disso.

- Sem suporte para backups contínuos sob demanda—AWS Backup não oferece suporte a backup contínuo sob demanda porque o backup sob demanda registra um point-in-time, enquanto os registros de backup contínuo mudam durante um período de tempo.
- Sem suporte para transição para armazenamento “frio”—os backups contínuos não oferecem suporte à transição para o armazenamento frio porque a transição para o frio requer um período de transição mínimo de 90 dias, enquanto os backups contínuos têm um período de retenção máximo de 35 dias.

Criando backups do Windows VSS

com AWS Backup, você pode fazer backup e restaurar aplicativos Windows habilitados para VSS (Volume Shadow Copy Service) em execução em instâncias do Amazon EC2. Você pode executar restaurações consistentes, usando o mesmo serviço de backup gerenciado usado para proteger outros AWS recursos da AWS. Com backups do Windows consistentes com aplicativos no EC2, você obtém as mesmas configurações de consistência e reconhecimento de aplicativos que as ferramentas tradicionais de backup.

Note

AWS Backup atualmente só suporta backups consistentes com aplicativos de recursos em execução no Amazon EC2. Nem todos os tipos de instância ou aplicativos são suportados para backups do Windows VSS.

Para obter mais informações, consulte [Criar um snapshot consistente com aplicativo do VSS](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Para fazer backup e restaurar recursos do Windows habilitados para VSS executando o Amazon EC2, siga estas etapas:

- Conclua as tarefas de pré-requisitos necessárias. Para obter instruções, consulte [Antes de começar](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.
- Faça download, instale e configure o agente VSS no AWS Systems Manager. Essa etapa é necessária. Para obter instruções, consulte [Atualizar o SSM Agent usando o Run Command](#) no AWS Guia do usuário do Systems Manager.
- Adicione uma política do IAM à função do IAM e anexe-a à instância do Amazon EC2 antes de fazer o backup do Windows VSS (Volume Shadow Copy Service). Para obter instruções, consulte [Como criar uma função do IAM para snapshots habilitados para VSS](#) no Guia do usuário do Amazon EC2 para instâncias do Windows. Para obter um exemplo de política do IAM, consulte [Políticas gerenciadas](#) (p. 104).
- Ativar VSS no AWS Backup.

Para ativar a cópia de segurança do Windows VSS no AWS Backup

1. Abrir o AWS Backup console do <https://console.aws.amazon.com/backup>.
2. No painel, escolha o tipo de backup que você deseja criar, ou [Criar um backup sob demanda](#) ou [Gerenciar planos de backup](#). Forneça as informações necessárias para o seu tipo de backup.
3. Quando você estiver atribuindo recursos, escolha EC2. Atualmente, o backup do Windows VSS é suportado apenas para instâncias do EC2.
4. No [Configurações avançadas](#), selecione VSS do Windows. Isso permite que você faça backups do Windows VSS consistentes com aplicativos.
5. Crie seu backup.

Instâncias do Amazon EC2 não compatíveis

Os seguintes tipos de instância do Amazon EC2 não são compatíveis com backups do Windows habilitados para VSS porque eles são instâncias pequenas e podem não fazer o backup com êxito.

- t3.nano
- t3.micro
- t3a.nano
- t3.micro
- t2.nano
- t2.micro

Como criar backups consistentes com falhas e multivolume do Amazon EBS

Por padrão, o AWS Backup cria backups consistentes com falhas dos volumes do Amazon EBS que estão conectados a uma instância do Amazon EC2. A consistência de falha significa que os snapshots de cada volume do Amazon EBS anexado à mesma instância do Amazon EC2 são obtidos exatamente no mesmo momento. Você não precisa mais interromper suas instâncias ou coordenar entre vários volumes do Amazon EBS para garantir a consistência de falhas do estado do aplicativo.

Como os snapshots de vários volumes e consistentes com falhas são um valor predefinido do AWS Backup, não é necessário fazer nada diferente para usar esse recurso. Você pode fazer backup de volumes do Amazon EBS usando um dos procedimentos a seguir:

- [Criar um backup sob demanda](#)
- [Criar um backup agendado](#)

Para restaurar seus volumes do Amazon EBS, siga as etapas em [Restaurar um volume do Amazon EBS](#).

Copiar tags em backups

Em geral, o AWS Backup copia tags dos recursos que ele protege para o seu ponto de recuperação. Ele não copia tags de seus pontos de recuperação para os recursos restaurados.

Por exemplo, quando você faz backup de um volume do Amazon EC2, o AWS Backup copia suas tags de recursos individuais e de grupo para o snapshot resultante, sujeito ao 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 \(p. 102\)](#).
- As tags originalmente associadas originalmente a um recurso e as marcações atribuídas durante o backup são atribuídas a pontos de recuperação armazenados em um cofre de backup, até no máximo 50 (esse é um limite AWS). As tags atribuídas durante o backup têm prioridade, e os dois conjuntos de tags são copiados em ordem alfabética.
- O DynamoDB não oferece suporte à atribuição de tags a backups. O AWS Backup não copia tags de tabelas.
- Os volumes do Amazon EBS anexados às instâncias do Amazon EC2 são recursos aninhados. As tags nos volumes do Amazon EBS anexados às instâncias do Amazon EC2 são tags aninhadas. O AWS Backup faz uma tentativa de melhor esforço para copiar tags aninhadas, mas se não for bem-sucedida, ele cria um backup sem elas e relata `Status Completed`.
- Quando um backup do Amazon EC2 cria um ponto de recuperação de imagem e um conjunto de snapshots, o AWS Backup copia tags para a AMI do resultante. O AWS Backup também faz a melhor tentativa de copiar as tags dos volumes associados à instância do Amazon EC2 para os snapshots resultantes.

Se você copiar seu backup para outra região AWS, o AWS Backup copia todas as tags do backup original para o destino AWS :

Interromper um trabalho de backup

Você pode interromper um trabalho de backup no AWS Backup depois que ele foi iniciado. 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 do <https://console.aws.amazon.com/backup>.
2. No painel de navegação à esquerda, escolha Jobs (Trabalhos).
3. Escolha o trabalho de backup que você deseja interromper.
4. No painel de detalhes do trabalho de backup, escolha Stop (Interromper).

Copiar um backup

Você pode copiar backups para várias AWS contas ou AWS Regiões sob demanda ou automaticamente como parte de um plano de backup programado. Você também pode automatizar uma sequência de cópias entre contas e regiões para a maioria dos recursos suportados, exceto para Amazon RDS e Aurora. Para snapshots do Amazon RDS e Aurora, AWS Backup oferece suporte somente à automação de cópias entre regiões devido à forma como esses serviços criam suas chaves de criptografia.

As cópias herdam sua configuração de origem, a menos que você especifique o contrário. Há uma exceção: se você especificar que sua cópia “Nunca” expirará, sua cópia ainda herdará sua data de expiração de origem. Atualmente, se você quiser que suas cópias de backup sejam permanentes, defina seus backups de origem para nunca expirarem ou especifique sua cópia para expirar 100 anos após sua criação.

Tópicos

- [Criação de cópias de backup em AWS Regiões da](#) (p. 49)
- [Criação de cópias de backup em AWS contas](#) (p. 51)

Criação de cópias de backup em AWS Regiões da

O uso do AWS Backup, você pode copiar backups para várias AWS Regiões sob demanda ou automaticamente como parte de um plano de backup programado. 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 obter um tutorial em vídeo, consulte [Gerenciamento de cópias entre regiões de backups](#).

Quando você copia um backup para um novo AWS Região pela primeira vez, o AWS Backup copia o backup na íntegra. Se um serviço oferecer suporte a backups incrementais, as cópias subsequentes desse backup na mesma AWS região será incremental. O AWS Backup criptografará novamente sua cópia usando a chave gerenciada pelo cliente do cofre de destino.

Você pode usar o AWS Backup para copiar seus backups para todos os compatíveis, definindo diferentes planos de backup em regiões diferentes, sujeito às seguintes limitações:

- O DynamoDB não oferece suporte a backup entre regiões.
- O Amazon RDS e o Aurora suportam backup entre regiões ou backup entre contas, mas não ambos no mesmo plano de backup. Você pode usar um AWS Lambda para realizar ambos. Além disso, copiando grupos de opções personalizadas do Amazon RDS em AWS Regiões não são compatíveis.

- O Amazon EFS oferece suporte à cópia entre regiões no nível do plano. Para aplicar uma regra de cópia diferente a um subconjunto de sistemas de arquivos, crie um novo plano.

Backup entre regiões estão disponíveis em todos os AWS Regiões disponíveis no AWS Backup. Exceto: Ásia-Pacífico (Hong Kong), Oriente Médio (Bahrein), Europa (Milão) e África (Cidade do Cabo).

Execução de backup entre regiões sob demanda

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 um cofre e escolha um ponto de recuperação no cofre.
4. Escolha o botão Copiar.
5. Insira os seguintes valores:

Região de destino

Escolha o destino do AWS Região da cópia. Você pode adicionar uma nova regra de cópia por cópia em um novo destino.

Note

Copiando tabelas do Amazon DynamoDB em AWS Regiões não são compatíveis.

(Configurações avançadas) Cofre de backup

Escolha o cofre de backup de destino para a cópia.

(Configurações avançadas) Função do IAM

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

(Configurações avançadas) Ciclo de vida

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.

Atualmente, apenas os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio". A expressão de armazenamento frio é ignorada para os backups do Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Aurora, Amazon DynamoDB e AWS Storage Gateway.

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.

6. Escolha Criar backup.

Agendar backup entre regiões

Você pode usar um plano de backup agendado para copiar backups em AWS Regiões.

Para copiar um backup usando um plano de backup agendado

1. Abrir oAWS Backupconsole do<https://console.aws.amazon.com/backup>.
2. DentroMinha conta, escolhaPlanos de backup, depois, escolhaCriar plano de backup.
3. NoCriar plano de backup, escolhaCriar um novo plano.
4. para oNome do plano de backupInsira um nome para o plano de backup.
5. NoConfiguração da regra de backupAdicione uma regra de backup que defina uma programação de backup, uma janela de backup e as regras do ciclo de vida. Você pode adicionar mais regras de backup mais tarde.

para oRule name (Nome da regra)Insira um nome para a regra.

6. NoScheduleSeção emFrequência, escolha a frequência com que você deseja que o backup seja feito.
7. para oJanela de backup, escolhaUsar padrões da janela de backup(recomendado). É possível personalizar a janela de backup.
8. para oCofre de backupEscolha um cofre na lista. Os pontos de recuperação para este backup serão salvos neste cofre. Crie um cofre de backup.
9. NoGerar cópia - opcionalInsira os seguintes valores:

Região de destino

Escolha o destino doAWSRegião da cópia de backup. Seu backup será copiado para esta região. Você pode adicionar uma nova regra de cópia por cópia em um novo destino.

Note

Copiando tabelas do Amazon DynamoDB emAWSRegiões não são compatíveis.

Copiar para o cofre de outra conta

Não alterne esta opção. Para saber mais sobre a cópia entre contas, consulte[Criação de cópias de backup emAWScontas](#)

Cofre de backup de destino

Selecione o cofre de backup na região de destino em que oAWS Backupirá copiar o seu backup.

Se você quiser criar um novo cofre de backup para cópia entre regiões, escolhaCriar um novo cofre de backup. Insira as informações no assistente. Em seguida, escolhaCriar cofre de backup.

10. SelecioneCriar plano.

Criação de cópias de backup emAWScontas

O uso doAWS Backup, você pode fazer backup de até váriosAWSContas sob demanda ou automaticamente como parte de um plano de backup programado. Use um backup entre contas se quiser copiar com segurança seus backups para um ou maisAWSem sua organização por motivos operacionais ou de segurança. Se o backup original for excluído inadvertidamente, você poderá copiar o backup de sua conta de destino para sua conta de origem e, em seguida, iniciar a restauração. Antes que você possa fazer isso, você deve ter duas contas que pertencem à mesma organização noAWS OrganizationsServiço do. Para obter mais informações, consulte[Tutorial: Como criar e configurar uma organização](#)noGuia do usuário das Organizations.

Na sua conta de destino, você deve criar um cofre de backup. Em seguida, atribua uma chave gerida pelo cliente para encriptar cópias de segurança na conta de destino e uma política de acesso baseada em recursos para permitirAWS Backuppara acessar os recursos que você gostaria de copiar. Na conta de origem, se seus recursos forem criptografados com uma chave gerenciada pelo cliente, você deverá compartilhar essa chave gerenciada pelo cliente com a conta de destino. Em seguida, você pode criar um

plano de backup e escolher uma conta de destino que faça parte de sua unidade organizacional no AWS Organizations.

Você pode usar o AWS Backup para copiar os backups de todos os recursos compatíveis, sujeito às seguintes limitações:

- O DynamoDB não oferece suporte ao backup entre contas.
- Para todos os serviços, exceto o Amazon EFS, o backup entre contas suporta apenas chaves gerenciadas pelo cliente. Ele não suporta cofres que são criptografados usando AWS, incluindo cofres padrão, porque AWS não se destina a ser compartilhadas entre contas.

Você deve usar cofres diferentes dos cofres padrão para executar backup entre contas.

Para o Amazon EFS, você pode executar backups entre contas usando qualquer cofre de backup do Amazon EFS porque AWS Backup gerencia de forma independente a criptografia para cada cofre de backup do Amazon EFS.

- O Amazon RDS e o Aurora suportam backup entre regiões ou backup entre contas, mas não ambos no mesmo plano de backup. Você pode usar um AWS Lambda para realizar ambos. Além disso, copiando grupos de opções personalizadas do Amazon RDS em AWS, regiões não são compatíveis.
- O Amazon EC2 não permite cópias entre contas do AWS IAMs do Marketplace. Para obter mais informações, consulte [Cópia de uma AMI](#) no Guia do usuário do Amazon EC2.

Backup entre regiões estão disponíveis em todos os AWS regiões disponíveis no AWS Backup. Exceto: Regiões China, Ásia-Pacífico (Hong Kong), Oriente Médio (Bahrein), Europa (Milão), África (Cidade do Cabo) e Ásia-Pacífico (Tóquio).

Configurar backup entre contas

O que você precisa para criar backups entre contas?

- Uma conta de origem

A conta de origem é a conta onde sua produção AWS reside recursos e backups primários.

O usuário da conta de origem inicia a operação de backup entre contas. O usuário ou função da conta de origem deve ter permissões de API apropriadas para iniciar a operação. As permissões apropriadas podem ser as AWS políticas gerenciadas `AWSBackupFullAccess`, o que permite acesso total ao AWS Operações de backup ou uma política gerenciada pelo cliente, como `ec2:ModifySnapshotAttribute`. Para obter mais informações sobre ambos os tipos de política, consulte [AWS Backup políticas gerenciadas pela](#).

- Uma conta de destino

A conta de destino é a conta onde você gostaria de manter uma cópia de seu backup. Você pode 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 `backup:CopyIntoBackupVault` para obter o seu cofre de backup de destino. A ausência desta política negará tentativas de cópia para a conta de destino.

- Uma conta de gerenciamento no AWS Organizations

A conta de gerenciamento é a conta principal em sua organização, conforme definido por AWS Organizations, que você usa para gerenciar o backup entre contas em seu AWS Contas. Você também precisa habilitar a confiança de serviço para usar o backup entre contas. Depois de habilitar a confiança de serviço, você pode usar qualquer conta na organização como uma conta de destino. Na sua conta de destino, você pode escolher quais cofres usar para backup entre contas.

- Habilite o backup entre contas no AWS Backup console

Para obter informações sobre segurança, consulte [Consideração de segurança para backup de contas cruzadas \(p. 59\)](#).

Para utilizar a cópia de segurança entre contas, tem de activar a funcionalidade de cópia de segurança entre contas. Em seguida, você deve “Permitir” a política de acesso `backup:CopyIntoBackupVault` em seu cofre de backup de destino.

Como habilitar o backup entre contas

1. Faça login em AWS. Usar a sua AWS Organizations Credenciais da conta de gerenciamento. A cópia de segurança entre contas só pode ser activada ou desactivada utilizando estas credenciais.
2. Abrir o AWS Backup console do <https://console.aws.amazon.com/backup>.
3. Dentro Minha conta, escolha Configurações.
4. para o Backup entre contas, escolha Habilitar o.
5. Dentro Cofres de backup, escolha o seu cofre de destino.
6. No Política de acesso seção, “Permitir” `backup:CopyIntoBackupVault`. Para obter um exemplo, selecione Adicionar permissões, em seguida Permitir acesso a um Cofre de backup da organização.
7. Agora, qualquer conta em sua organização pode compartilhar o conteúdo de seu cofre de backup com qualquer outra conta em sua organização. Para obter mais informações, consulte [Compartilhando um cofre de backup com outro AWS account \(p. 56\)](#). Para limitar quais contas podem receber o conteúdo dos cofres de backup de outras contas, consulte [Configurando sua conta como uma conta de destino \(p. 58\)](#).

Agendar backup entre contas

Você pode usar um plano de backup agendado para copiar backups em AWS contas.

Para copiar um backup usando um plano de backup agendado

1. Abrir o AWS Backup console do <https://console.aws.amazon.com/backup>.
2. Dentro Minha conta, escolha Planos de backup, depois, escolha Criar plano de backup.
3. No Criar plano de backup, escolha Criar um novo plano.
4. para o Nome do plano de backup Insira um nome para o plano de backup.
5. No Configuração da regra de backup Adicione uma regra de backup que defina uma programação de backup, uma janela de backup e as regras do ciclo de vida. Você pode adicionar mais regras de backup mais tarde.

para o Rule name (Nome da regra) Insira um nome para a regra.
6. No Schedule Seção em Frequência, escolha a frequência com que você deseja que o backup seja feito.
7. para o Janela de backup, escolha Usar padrões da janela de backup (recomendado). É possível personalizar a janela de backup.
8. para o Cofre de backup Escolha um cofre na lista. Os pontos de recuperação para este backup serão salvos neste cofre. Crie um cofre de backup.
9. No Gerar cópia - opcional Insira os seguintes valores:

Região de destino

Escolha o destino do AWS Região da cópia de backup. Seu backup será copiado para esta região. Você pode adicionar uma nova regra de cópia por cópia em um novo destino.

Note

Copiando tabelas do Amazon DynamoDB em AWS Regiões não são compatíveis.

Copiar para o cofre de outra conta

Altere para escolher esta opção. A opção fica azul quando selecionada. O ARN do cofre externoserá exibida.

ARN do cofre externo

Insira o nome de recurso da Amazon (ARN) da conta de destino. O ARN é uma string que contém o ID da conta e suaAWSRegião :AWS Backupcopiará o backup para o cofre da conta de destino. ORegião de destinoatualiza automaticamente para a Região no ARN do cofre externo.

para oPermitir o acesso ao cofre de backup, escolhaPermitir. Em seguida, escolhaPermitirno assistente que é aberto.

AWS Backupprecisa de permissões para acessar a conta externa para copiar o backup para o valor especificado. O assistente mostra a seguinte política de exemplo 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"
      }
    }
  ]
}
```

(Configurações avançadas) Transição para armazenamento frio (somente para EFS)

Escolha as opções que você deseja para o seu sistema de arquivos EFS.

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.

Atualmente, apenas os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio". A expressão de armazenamento frio é ignorada para os backups do Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Aurora, Amazon DynamoDB eAWS Storage Gateway.

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 expirarem e estiverem marcados para exclusão como parte de sua política de ciclo de vida,AWS Backupexclui os backups em um ponto escolhido aleatoriamente ao longo das 8 horas seguintes. Essa janela ajuda a garantir um desempenho consistente.

10. SelecioneMarcas adicionadas aos pontos de recuperaçãopara adicionar tags aos seus pontos de recuperação.
11. para oConfigurações avançadas de backup, escolhaVSS do Windowspara habilitar snapshots com reconhecimento de aplicativo para o software de terceiros selecionado em execução no EC2.
12. SelecioneCriar plano.

Execução de backup entre contas sob demanda

Você pode copiar um backup para uma AWS Conta sob demanda.

Como copiar um backup sob demanda

1. Abrir o AWS Backup console do <https://console.aws.amazon.com/backup>.
2. Para a minha conta, escolha Cofre de backup para ver todos os seus cofres de backup listados. Você pode filtrar pelo nome ou etiqueta do cofre de backup.
3. Selecione o ID do ponto de recuperação do backup que você deseja copiar.
4. Escolha Copiar.
5. Ampliar Detalhes do backup para ver informações sobre o ponto de recuperação que você está copiando.
6. No Copiar configuração Escolha uma opção na lista de Região de destino Lista do.
7. Selecione Copiar para o cofre de outra conta. A opção fica azul quando selecionada.
8. Insira o nome de recurso da Amazon (ARN) da conta de destino. O ARN é uma string que contém o ID da conta e sua AWS Região: AWS Backup copiará o backup para o cofre da conta de destino. O Região de destino atualiza automaticamente para a Região no ARN do cofre externo.
9. Para o Permitir acesso ao cofre de backup, escolha Permitir. Em seguida, escolha Permitir no assistente que é aberto.

AWS Backup precisa de permissões para acessar a conta externa (origem). O assistente mostra um 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. (Somente Amazon EFS) Para transição para armazenamento a frio, escolha as opções desejadas para o seu sistema de arquivos EFS.

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.

Atualmente, apenas os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio". A expressão do armazenamento "frio" é ignorada para os backups do Amazon EBS, Amazon RDS, Amazon Aurora, Amazon DynamoDB e AWS Storage Gateway.

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. Para o IAM role (Função do IAM), especifique a função do IAM (como a função padrão) que tem as permissões para disponibilizar o backup para cópia. O ato de copiar é realizado pela função vinculada ao serviço da conta de destino.

12. Escolha Copiar. Dependendo do tamanho do recurso que você está copiando, esse processo pode levar várias horas para ser concluído. Quando o trabalho de cópia for concluído, você verá a cópia no Copiar trabalhos Guias do Trabalhos domenu.

Restaurando um backup de uma AWS conta para outra

AWS Backup não oferece suporte à recuperação de recursos de uma AWS para outra conta. No entanto, pode copiar uma cópia de segurança de uma conta para outra e, em seguida, restaurá-la nessa conta. Por exemplo, não é possível restaurar uma cópia de segurança da conta A para a conta B, mas pode copiar uma cópia de segurança da conta A para a conta B e, em seguida, restaurá-la na conta B.

Restaurar um backup de uma conta para outra é um processo de duas etapas.

Para restaurar um backup de uma conta para outra

1. Copie o backup da origem AWS para a conta que você deseja restaurar. Para obter instruções, consulte [Criação de cópias de backup em AWS contas](#) (p. 51).
2. Use as instruções apropriadas para seu recurso para restaurar o backup.

Compartilhando um cofre de backup com outra AWS account

AWS Backup permite que você compartilhe um cofre de backup com uma ou várias contas, ou toda a sua organização no AWS Organizations. Você pode compartilhar um cofre de backup de destino com uma fonte AWS conta, usuário ou função do IAM.

Para compartilhar um Cofre de backup de destino

1. Selecione AWS Backup, depois, escolha Cofres de backup.
2. Escolha o nome do cofre de backup que você deseja compartilhar.
3. No Política de acesso, selecione o Adicionar permissões Dropdown.
4. Selecione Permitir acesso em nível de conta a um Cofre de backup. Ou, você pode optar por permitir acesso em nível de organização ou em nível de função.
5. Digite o Account ID da conta que você gostaria de compartilhar com este Cofre de backup de destino.
6. Selecione Salvar política.

Você pode usar as políticas do IAM para compartilhar seu cofre de backup.

- [Compartilhe um cofre de backup de destino com uma AWS conta ou função do IAM](#) (p. 56)
- [Compartilhar um cofre de backup de destino em uma unidade organizacional no AWS Organizations](#) (p. 57)
- [Compartilhe um cofre de backup de destino com uma organização no AWS Organizations](#) (p. 57)

Compartilhe um cofre de backup de destino com uma AWS conta ou função do IAM

A política a seguir compartilha um cofre de backup com o número da conta 444455556666 e a função do IAM SomeRole no número da 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": "*"
  }
]
```

Compartilhar um cofre de backup de destino em uma unidade organizacional noAWS Organizations

A política a seguir compartilha um cofre de backup com unidades organizacionais usando seusPrincipalOrgPaths.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringLike": {
          "aws:PrincipalOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/ou-jkl0-awsdddddd/*"
          ]
        }
      }
    }
  ]
}
```

Compartilhe um cofre de backup de destino com uma organização noAWS Organizations

A política a seguir compartilha um cofre de backup com a organização comPrincipalOrgID "o-a1b2c3d4e5".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": [
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

Configurando sua conta como uma conta de destino

Quando você habilita os backups entre contas pela primeira vez usando o AWS Organizations, qualquer usuário de uma conta de membro pode configurar sua conta para ser uma conta de destino. Recomendamos definir um ou mais dos seguintes controles de acesso no AWS Organizations para limitar suas contas de destino.

- [Limitar contas de destino usando tags \(p. 58\)](#)
- [Limitar contas de destino usando números de conta e nomes de cofre \(p. 58\)](#)
- [Limitar contas de destino usando unidades organizacionais no AWS Organizations \(p. 58\)](#)

Limitar contas de destino usando tags

A política a seguir limita as contas de destino a contas com cofres de backup marcados `DestinationBackupVault`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/DestinationBackupVault": "true"
        }
      }
    }
  ]
}
```

Limitar contas de destino usando números de conta e nomes de cofre

A política a seguir limita as contas de destino a apenas duas contas. A primeira conta de destino é a conta `112233445566` com o prefixo de nome do cofre de backup `cab`. A segunda conta de destino é a conta `123456789012` em AWS Região `us-west-1` com 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"
          ]
        }
      }
    }
  ]
}
```

Limitar contas de destino usando unidades organizacionais no AWS Organizations

A política a seguir limita as contas de destino às contas dentro de determinadas unidades organizacionais. É preciso anexar essa política a umAWS Organizationsque contém sua conta de origem.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "backup:CopyFromBackupVault",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringNotLike": {
          "backup:CopyTargetOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/ou-jkl0-awsdddddd/*"
          ]
        }
      }
    }
  ]
}
```

Consideração de segurança para backup de contas cruzadas

Esteja ciente do seguinte ao usar a execução de backups entre contas noAWS Backup:

- O cofre de destino não pode ser o cofre padrão. Isso ocorre porque o cofre padrão é criptografado com uma chave que não pode ser compartilhada com outras contas.
- Os backups entre contas ainda podem ser executados por até 15 minutos após você desativar o backup entre contas. Isso se deve a uma consistência eventual e pode resultar em alguns trabalhos entre contas iniciando ou concluídos mesmo depois que você desabilita o backup entre contas.
- Se a conta de destino deixar a organização em uma data posterior, essa conta manterá os backups. Para evitar possíveis vazamentos de dados, coloque uma permissão de negação no `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 de sua organização](#) no Guia do usuário das Organizations.
- Se você excluir uma função de trabalho de cópia durante uma cópia de conta cruzada, AWS Backup não pode cancelar o compartilhamento de snapshots da conta de origem quando o trabalho de cópia for concluído. Nesse caso, o trabalho de backup é concluído, mas o status do trabalho de cópia é exibido como Falha ao cancelar o compartilhamento do snapshot.

Visualizar uma lista de backups

Há duas maneiras de visualizar uma lista dos seus backups usando o console do AWS Backup. Você pode visualizar os backups associados a umAWS recurso. Ou, você pode visualizar todos os backups que são organizados em um único cofre de backup, que pode estar em váriosAWS recursos e diferentes tipos de recursos.

Tópicos

- [Listando backups por recurso protegido \(p. 59\)](#)
- [Listando backups por cofre de backup \(p. 60\)](#)

Listando backups por recurso protegido

Siga estas etapas para exibir uma lista de backups de um recurso específico no console do AWS Backup.

1. Faça login noAWS Management Consolee abra oAWS Backupconsole do<https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolha Protected resources (Recursos protegidos).
3. Escolha um recurso protegido na lista para visualizar a lista de backups. Apenas os recursos submetidos a backup pelo AWS Backup estão listados na página Protected resources (Recursos protegidos).

É possível visualizar todos os backups do recurso, mesmo aqueles que não foram criados pelo AWS Backup. Nesta tela, você também pode escolher um backup e restaurá-lo.

Listando backups por cofre de backup

Siga estas etapas para exibir uma lista de backups organizados em um cofre de backup.

1. Abrir oAWS Backupconsole do<https://console.aws.amazon.com/backup>.
2. No painel de navegação, selecione Backup vaults (Cofres de backup).
3. Na seção Backups, visualize a lista de todos os backups organizados neste cofre de backup. Nesta tela, você pode selecionar um backup e editá-lo, excluí-lo ou restaurá-lo.

Editar um backup

Depois de criar um backup usando o AWS Backup, você pode alterar o ciclo de vida ou 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.

Atualmente, apenas os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio". A expressão de armazenamento frio é ignorada para os backups do Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Aurora, Amazon DynamoDB eAWS Storage Gateway.

Note

Editando as tags de um backup usandoAWS BackupO é compatível apenas com backups dos sistemas de arquivos do Amazon Elastic File System (Amazon EFS). Você ainda pode editar as tags de outros serviços de backups 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 "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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 noAWS Management Consolee abra oAWS Backupconsole do<https://console.aws.amazon.com/backup>.
2. No painel de navegação, selecione Backup vaults (Cofres de backup).

3. Na seção Backups, selecione um backup.
4. Na página de detalhes do backup, selecione Edit (Editar).
5. Defina as configurações de ciclo de vida e escolha Save (Salvar).

Restaurar um backup

Quando você restaure um backup no AWS Backup, geralmente, ele cria um novo recurso com base no backup que você está restaurando. Para cada restauração, você deve especificar os parâmetros de restauração.

Os parâmetros de restauração são específicos a um tipo de recurso, como o tamanho do volume ao restaurar um snapshot do Amazon Elastic Block Store (Amazon EBS). Quando você restaura um backup usando o console do AWS Backup, os parâmetros de restauração específicos do serviço são apresentados automaticamente. Para cada restauração, um trabalho de restauração é criado com um ID de trabalho exclusivo — por exemplo, `1323657E-2AA4-1D94-2C48-5D7A423E7394`.

Você pode visualizar o status de um trabalho de restauração na [Página do AWS Backup console](#). Os status do trabalho de restauração incluem: criado, pendente, em execução, cancelando, cancelado, concluído, falhou e expirado.

Para obter instruções básicas de restauração e links para a documentação de cada serviço que usa o console AWS Backup, consulte [Restaurar um backup](#) (p. 24) na seção Introdução.

Para restaurar um backup usando o AWS Command Line Interface (AWS CLI) normalmente, a API ou o SDK, você precisa passar informações de configuração do recurso para o `StartRestoreJob` (p. 330) Operação da API.

As informações de configuração que você precisa para restaurar seu recurso varia de acordo com o serviço que você deseja restaurar. Para obter os metadados de configuração com os quais o backup foi criado, chame `GetRecoveryPointRestoreMetadata` (p. 279), mas podem ser necessárias informações adicionais para restaurar o recurso. Cada serviço requer diferentes valores de configuração para restaurar um ponto de recuperação.

Tópicos

- [Restaure um sistema de arquivos do Amazon FSx](#) (p. 61)
- [O uso do AWS Backup para restaurar um volume do Amazon EBS](#) (p. 65)
- [Restaurar um sistema de arquivos do Amazon EFS](#) (p. 66)
- [Restaurando um banco de dados do Amazon DynamoDB](#) (p. 69)
- [Restaurar um banco de dados do Amazon RDS](#) (p. 70)
- [Restaure um cluster do Amazon Aurora](#) (p. 72)
- [Restaure uma instância do Amazon EC2](#) (p. 74)
- [Restaurar uma AWS Storage Gateway volume](#) (p. 76)
- [Usar o AWS Backup API, CLI ou SDK para restaurar pontos de recuperação do Amazon EC2](#) (p. 76)

Restaure um sistema de arquivos do Amazon FSx

As opções de restauração que estão disponíveis quando você usa o AWS Backup para restaurar os sistemas de arquivos do Amazon FSx são os mesmos que usar o backup nativo do Amazon FSx. É possível usar o ponto de recuperação do backup para criar um novo sistema de arquivos e restaurar um snapshot point-in-time de outro sistema de arquivos.

Ao restaurar sistemas de arquivos do Amazon FSx, o AWS Backup cria um novo sistema de arquivos e o preenche com os dados. 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 novo sistema de arquivos. Os dados restaurados a partir do backup são carregados lentamente no sistema de arquivos. Você pode, portanto, enfrentar uma latência ligeiramente maior durante o processo.

Note

Você não pode restaurar para um sistema de arquivos do Amazon FSx existente e não pode restaurar arquivos ou pastas individuais.

AWS Backup cofres que contêm pontos de recuperação dos sistemas de arquivos do Amazon FSx são visíveis fora do AWS Backup. Você pode restaurar os pontos de recuperação usando o Amazon FSx, mas não pode excluí-los.

Você pode ver os backups criados pela funcionalidade interna de backup automático do Amazon FSx a partir do AWS Backup console. Você também pode recuperar esses backups usando AWS Backup. No entanto, você não pode excluir esses backups ou alterar as programações de backup automático de seus sistemas de arquivos Amazon FSx usando AWS Backup.

É possível restaurar backups criados pelo AWS Backup usando o AWS Backup console, a API do AWS CLI. Esta seção explica como usar o AWS Backup para restaurar sistemas de arquivos do Amazon FSx.

Usar o AWS Backup console para restaurar pontos de recuperação do Amazon FSx

Restaurando um sistema de arquivos do Amazon FSx for Windows File Server

Para restaurar um sistema de arquivos do Amazon FSx for Windows File Server

1. Abrir o AWS Backup console em <https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolha Recursos protegidos. Em seguida, escolha o ID de recurso do Amazon FSx que você deseja restaurar.
3. Na página Resource details (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 o Restaurar backup.
5. No Detalhes do sistema de arquivos, o ID do seu backup é mostrado em ID de backup, e o tipo de sistema de arquivos é mostrado em Tipo de sistema de arquivos. Você pode restaurar o Amazon FSx for Windows File Server e o Amazon FSx for Lustre sistemas de arquivos.
6. (Opcional) Insira um nome para o sistema de arquivos.
7. para o Tipo de implantação, aceite o padrão. Não é possível alterar o tipo de implantação de um sistema de arquivos durante a restauração.
8. Selecione o Tipo de armazenamento para usar. Se a capacidade de armazenamento do seu sistema de arquivos for inferior a 2.000 GiB, você não poderá usar o HDD Tipo de armazenamento.
9. para a Capacidade de throughput, escolha Capacidade de taxa de transferência recomendada para usar a taxa recomendada de 16 MB/s ou escolha Especificar capacidade de throughput insira uma nova taxa.
10. No Rede e segurança, forneça as informações necessárias.
11. Se você estiver restaurando um sistema de arquivos do Amazon FSx for Windows File Server, forneça a Autenticação Utilizadas para acessar o sistema de arquivos ou então você pode criar um novo.

Note

Ao restaurar uma cópia de segurança, não é possível alterar o tipo de Active Directory no sistema de arquivos.

Para obter mais informações sobre o Microsoft Active Directory, consulte [Trabalhando com o Active Directory no Amazon FSx for Windows File Server](#) no Guia do usuário do Amazon FSx for Windows File Server.

12. (Opcional) Na caixa de diálogo Backup e manutenção Forneça as informações para definir suas preferências de backup.
13. No Função de restauração Escolha a função do IAM do que o AWS Backup O usará para criar e gerenciar seus backups em seu nome. Recomendamos que você escolha a Função padrão. Se não houver nenhuma função padrão, uma será criada para você com as permissões corretas. Você também pode fornecer sua própria função do IAM.
14. Verifique todas as suas entradas e escolha Restaurar backup.

Restauração de um sistema de arquivos Amazon FSx for Lustre

AWS Backup suporta o Amazon FSx para sistemas de arquivos Lustre que têm tipo de implantação de armazenamento persistente e não estão vinculados a um repositório de dados como o Amazon S3.

Para restaurar um sistema de arquivos do Amazon FSx for Lustre

1. Abra o AWS Backup console do <https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolha Recursos protegidos E, em seguida, escolha o ID de recurso do Amazon FSx que você deseja restaurar.
3. Na página Resource details (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 o Restaurar o backup para o novo sistema de arquivos.
5. No Configurações, o ID do seu backup é mostrado em ID de backup, e o tipo de sistema de arquivos é mostrado em Tipo de sistema de arquivos. Tipo de sistema de arquivos deve ser Lustre.
6. (Opcional) Insira um nome para o sistema de arquivos.
7. Selecione Choose Tipo de implantação. AWS Backup suporta apenas o tipo de implementação 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 Amazon FSx for Lustre, consulte [Usando opções de implantação disponíveis para o Amazon FSx for Lustre](#) no Guia do usuário do Amazon FSx for Lustre.

8. Selecione a Taxa de transferência por unidade de armazenamento que você deseja usar.
9. Especifique a Capacidade de armazenamento para usar. Insira uma capacidade entre 32 GiB e 64.436 GiB.
10. No Rede e segurança, forneça as informações necessárias.
11. Se você estiver restaurando um sistema de arquivos do Amazon FSx for Windows File Server, forneça a Autenticação Informações usadas para acessar o sistema de arquivos ou criar um novo.

Para obter informações detalhadas sobre o Microsoft Active Directory, consulte [Trabalhando com o Active Directory no Amazon FSx for Windows File Server](#) no Guia do usuário do Amazon FSx for Windows File Server.

12. (Opcional) Na caixa de diálogo Backup e manutenção Forneça as informações para definir suas preferências de backup.
13. No Função de restauração Escolha a função do IAM do que o AWS Backup O usará para criar e gerenciar seus backups em seu nome. Recomendamos que você escolha a Função padrão. Se não houver nenhuma função padrão, uma será criada para você com as permissões corretas. Você também pode fornecer sua função do IAM.

14. Verifique todas as suas entradas e escolhaRestaurar backup.

Usar aAWS BackupAPI, CLI ou SDK para restaurar pontos de recuperação do Amazon FSx

Para restaurar o Amazon FSx usando a API ou a CLI, use[StartRestoreJob](#). Você pode especificar os metadados a seguir durante qualquer restauração do Amazon FSx:

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
```

Metadados de restauração do Amazon FSx for Windows File Server

É possível especificar os metadados a seguir durante uma restauração do Amazon FSx for Windows File Server:

```
ThroughputCapacity
PreferredSubnetId
ActiveDirectoryId
```

Metadados de restauração do Amazon FSx for Lustre

Você pode especificar os seguintes metadados durante uma restauração do Amazon FSx for Lustre:

```
PerUnitStorageThroughput
DriveCacheType
```

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 restauração de metadados:

```
"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\\\\"\\"]\\"}"
```

O uso do AWS Backup para restaurar um volume do Amazon EBS

Ao restaurar um snapshot do Amazon Elastic Block Store (Amazon EBS), o AWS Backup cria um novo volume do Amazon EBS que você pode anexar à sua instância do Amazon EC2.

Note

Quando você inicia uma restauração do Amazon EBS por meio do AWS Backup, ele criptografará o volume restaurado do Amazon EBS usando o AWS CMK gerenciado pela Amazon EBS por padrão.

Você pode optar por restaurar o snapshot como um volume do EBS ou como um AWS Storage Gateway volume do.

Usar o AWS Backup Console para restaurar pontos de recuperação do Amazon EBS

Para restaurar um volume do Amazon EBS

1. Abrir o AWS Backup console do <https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolha Recursos protegidos e escolha o ID de recurso do EBS que você deseja restaurar.
3. Na página Resource details (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.

para o Resource type (Tipo de recurso), escolha a opção AWS para criar ao restaurar esse backup.

5. Se você escolher EBS volume (Volume do EBS), forneça os valores para o Volume type (Tipo de volume), Size (GiB) (Tamanho) e escolha uma Availability zone (Zona de disponibilidade).

Se escolher Volume Storage Gateway, escolha um Gateway em um estado acessível. Escolha também o seu Nome do destino iSCSI.

- para o Volume armazenado em gateways, escolha um ID de disco.
 - para o Volume armazenado em cache, selecione uma capacidade que seja pelo menos tão grande quanto o seu recurso protegido.
6. para a Função de restauração, escolha a função do IAM que o AWS Backup assumirá para esta restauração.

Note

Se o AWS Backup não tiver uma função padrão na sua conta, uma função padrão é criada para você com as permissões corretas. Você pode excluir essa função padrão ou torná-la inutilizável.

7. Escolha Restore backup (Restaurar backup).

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

Usar aAWS BackupAPI, CLI ou SDK para restaurar pontos de recuperação do Amazon EBS

Para restaurar o Amazon EBS usando a API ou a CLI, use `StartRestoreJob`. Você pode especificar os metadados a seguir durante qualquer restauração do Amazon EBS:

```
volumeId  
encrypted  
kmsKey  
availabilityZone
```

Exemplo:

```
"restoreMetadata": "{\"encrypted\": \"false\", \"volumeId\": \"vol-04cc95f3490b5ceea\",  
\"availabilityZone\": null}"
```

Restaurar um sistema de arquivos do Amazon EFS

Se você estiver restaurando uma instância do Amazon Elastic File System (Amazon EFS), será possível 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.

Restauração em nível de item

Quando você executa uma restauração em nível de item, o AWS Backup restaura um arquivo ou um diretório específico. Você deve 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 letras maiúsculas de minúsculas. Curingas e strings regex não são compatíveis.

Você pode restaurar esses itens para um sistema de arquivos novo ou existente. Se você restaurar os itens para um sistema de arquivos existente, oAWS Backupcria 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.

Usar aAWS BackupConsole para restaurar um ponto de recuperação do Amazon EFS

Para restaurar um sistema de arquivos do Amazon EFS

1. Abrir oAWS Backupconsole do<https://console.aws.amazon.com/backup>.

2. Seu cofre de backup EFS recebe a política de acesso `Deny backup:StartRestoreJob` na criação. Se você estiver restaurando o cofre de backup pela primeira vez, será necessário 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 o cofre Política de acesso
 - d. Se estiver presente, exclua `backup:StartRestoreJob` do `Statement`. Faça isso escolhendo `Edit`, excluindo `backup:StartRestoreJob`, depois escolhendo `Salvar` política.
3. No painel de navegação, escolha `Recursos protegidos` e o ID do sistema de arquivos do EFS que você deseja restaurar.
4. No `Detalhes do recurso` Uma lista de pontos de recuperação para o ID de sistema de arquivos selecionado é mostrada. Para restaurar um sistema de arquivos, no `Backups` do `Selecione` 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 Full restore (Restauração completa), que restaura todo o sistema de arquivos. Ou, poderá restaurar arquivos e diretórios específicos usando a Restauração em nível de item.

- Selecione `Restauração completa` Para restaurar o sistema de arquivos na sua totalidade, 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. Você pode selecionar e restaurar até cinco itens no 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. Você pode selecionar e restaurar até cinco itens no Elastic File System.
6. Para Restore local (Restaurar local)
 - Selecione `Restaurar` para o diretório no sistema de arquivos de origem Se você deseja restaurar para o sistema de arquivos de origem.
 - Selecione `Restaurar` um novo sistema de arquivos Se você deseja restaurar para um sistema de arquivos diferente.
 7. para o Tipo de sistema de arquivos
 - (Recomendado) Escolha `Regional` se você deseja restaurar seu sistema de arquivos em vários `AWS Zonas` de disponibilidade.
 - Selecione `One Zone` se quiser restaurar o sistema de arquivos para uma única Zona de disponibilidade. Em seguida, no `Zona` de disponibilidade, escolha o destino para a restauração.

Para obter mais informações, consulte [Gerenciando classes de armazenamento do Amazon EFS](#) no Guia do usuário do Amazon EFS.

8. para o Desempenho
 - Se você optar por executar um `Regional` restaurar, escolha (Recomendado) `Propósito geral` ou `E/S máxima`.

- Se você optar por executar um `One Zone` restaurar, você deve escolher (Recomendado) `Propósito geral`. Restaurações de uma zona não suportam `E/S` máxima.
9. para o `Enable encryption` (Habilitar criptografia)
- Escolha `Ativar criptografia`, se desejar criptografar seu sistema de arquivos. IDs e aliases de chave do KMS aparecem na lista depois de terem sido criados usando o comando `AWS Key Management Service` (AWS KMS) console do.
 - No `Chave do KMS` em, escolha a chave que você deseja usar na lista.
10. para o `Função de restauração`, escolha a função do IAM que `AWS Backup` assumirá para esta restauração.

Note

Se o `AWS Backup` a função padrão do não estiver presente na sua conta, uma função padrão é criado para você com as permissões corretas. Você pode excluir essa função padrão ou torná-la inutilizável.

11. Escolha `Restore backup` (Restaurar backup).

O painel `Tarefas de restauração` é 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.

Usar a `AWS Backup API`, CLI ou SDK para restaurar pontos de recuperação do Amazon EFS

Use `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 precisa das seguintes informações:

- `file-system-id`— O ID do sistema de arquivos do Amazon EFS do que é submetido a backup pelo `AWS Backup`. Restaurado em `GetRecoveryPointRestoreMetadata`.
- `Encrypted`— Um valor booleano que, quando verdadeiro, especifica que o sistema de arquivos é criptografado. Se `KmsKeyId` for especificado, `Encrypted` deverá ser definido como `true`.
- `KmsKeyId`— Especifica o `AWS KMS` chave do que é usada para criptografar o sistema de arquivos restaurado.
- `PerformanceMode`— Especifica o modo de taxa de transferência do sistema de arquivos.
- `CreationToken`— um valor fornecido pelo usuário que garante a exclusividade (idempotência) da solicitação.
- `newFileSystem`— um valor booleano 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. Usar o `ItemsToRestore` Para restaurar arquivos ou diretórios específicos em vez de todo o sistema de arquivos. Esse parâmetro é opcional.

Para obter mais informações sobre valores de configuração do Amazon EFS, consulte [criar-sistema de arquivos](#).

Restaurando um banco de dados do Amazon DynamoDB

Usar aAWS BackupConsole para restaurar pontos de recuperação do DynamoDB

Como restaurar um banco de dados do DynamoDB

1. Abrir oAWS Backupconsole do<https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolhaRecursos protegidosE o ID de recurso do DynamoDB que você deseja restaurar.
3. Na página Resource details (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 Settings (Configurações), campo de textoNew table name (Novo nome de tabela), insira um novo nome de tabela.
5. para oFunção de restauração, escolha a função do IAM queAWS Backupassumirá para esta restauração.

Note

Se oAWS BackupA função padrão do não estiver presente na sua conta, umaFunção padrãoO é criado para você com as permissões corretas. Você pode excluir essa função padrão ou torná-la inutilizável.

6. Escolha Restore backup (Restaurar backup).

O painel Tarefas de restauração é 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.

Usar aAWS BackupAPI, CLI ou SDK para restaurar pontos de recuperação do DynamoDB

Use `StartRestoreJob`. Você pode especificar os metadados a seguir durante qualquer restauração do DynamoDB:

```
originalTableName  
backupName  
backupArn  
primaryPartitionKey  
sortKey  
provisionedRcu  
provisionedWcu  
encryptionType  
kmsMasterKeyArn  
autoScaling  
stream  
secondaryIndices
```

```
indexName
indexType
projectedAttributes
targetTableName
```

Exemplo:

```
"restoreMetadata": "{ \"provisionedWriteCapacityUnits\": \"0\", \"autoScaling\":  
  \"Disabled\", \"kmsMasterKeyArn\": \"Not Applicable\", \"encryptionType\": \"Default  
  \", \"provisionedReadCapacityUnits\": \"0\", \"secondaryIndices\": \"[ ]\", \"backupArn  
  \": \"arn:aws:dynamodb:us-east-1:234567890123:table/simcher-loadtest-ScenariosTable-  
  C4B1NQ3B92DU/backup/01616319501023-bc657c53\", \"sortKey\": \"-\", \"stream\": \"Disabled  
  \", \"targetTableName\": null, \"originalTableName\": \"simcher-loadtest-ScenariosTable-  
  C4B1NQ3B92DU\", \"backupName\": \"simcher-loadtest-ScenariosTable-C4B1NQ3B92DU-  
  AwsBackup-2021-03-21T09.15.00Z-D2A6E00C-F3F8-AD99-A47D-8AA26EA38F01\", \"primaryPartitionKey  
  \": \"testId\" }"
```

Restaurar um banco de dados do Amazon RDS

Restaurar um banco de dados do Amazon RDS exige especificar várias opções de restauração. Para obter mais informações sobre essas opções, consulte [Fazer backup e restaurar uma instância de banco de dados do Amazon RDS](#) no Guia do usuário do Amazon RDS.

Usar aAWS BackupConsole para restaurar pontos de recuperação do Amazon RDS

1. Abrir oAWS Backupconsole do<https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolhaRecursos protegidosE o ID de recurso do Amazon RDS que você deseja restaurar.
3. Na página Resource details (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 Instance specifications (Especificações de instância), aceite os valores predefinidos ou especifique as opções para as configurações de DB engine (Mecanismo de banco de dados),License Model (Modelo de licença), DB instance class (Classe de instância de banco de dados),Multi AZ e Storage type (Tipo de armazenamento).
5. NoConfiguraçõesEspecifique um nome exclusivo para todas as instâncias de banco de dados pertencentes ao seuAWSNa região da 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 Network & Security (Rede e segurança) aceite os valores predefinidos ou especifique as opções para a configurações de Virtual Private Cloud (VPN) (Nuvem privada virtual (VPN)), Subnet group (Grupo de subredes), Public Accessibility (Acessibilidade pública) (geralmente Sim) e Availability zone (Zona de disponibilidade).
7. No painel Database options (Opções de banco de dados), aceite os valores predefinidos ou especifique as opções para as configurações de Database port (Porta de banco, de dados), DB parameter group (Group de parâmetros de banco de dados), Option Group (Grupo de opções), Copy tags to snapshots (Copiar tags para snapshots), e IAM DB Authentication Enabled (Autenticação de banco de dados de IAM habilitada).
8. NoCriptografia, aceite os valores predefinidos ou especifique as opções para oCriptografiaeChave do KMSConfigurações do .
9. No painel Log exports (Exportação de logs), escolha os tipos de log a serem publicados no Amazon CloudWatch Logs. A IAM role (Função do IAM) já está definida.

10. No painel Maintenance (Manutenção), aceite o valor predefinido ou especifique a opção para Auto minor version upgrade (Atualização de versão secundária automática).
11. No painel de Restore role (Restaurar função), escolha a função do IAM que o AWS Backup assumirá para essa restauração.
12. Depois que todas as configurações tiverem sido especificadas, escolha Restore backup (Restaurar backup).

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

Usar aAWS BackupAPI, CLI ou SDK para restaurar pontos de recuperação do Amazon RDS

Use `StartRestoreJob`. Você pode especificar os metadados a seguir durante as restaurações do Amazon RDS:

```
String dbInstanceIdentifier;
String engine;
String licenseModel;
String dbInstanceClass;
String availabilityZone;
Boolean multiAZ;
Boolean publiclyAccessible;
String storageType;
Integer port;
Integer iops;
Boolean autoMinorVersionUpgrade;
String dbParameterGroupName;
String optionGroupName;
List<String> vpcSecurityGroupIds;
String dbSubnetGroupName;
Boolean enableIAMDatabaseAuthentication;
Boolean deletionProtection;
String dbName;
String tdeCredentialArn;
String domain;
String domainIAMRoleName;
Boolean copyTagsToSnapshot;
List<String> enableCloudwatchLogsExports;
List<ProcessorFeature> processorFeatures;
```

Exemplo:

```
"restoreMetadata": "{ \"LicenseModel\": \"postgresql-license\", \"StorageType\": \"gp2\", \"DBInstanceClass\": \"db.t2.small\", \"Port\": \"0\", \"AvailabilityZone\": \"us-east-1d\", \"OptionGroupName\": \"default:postgres-12\", \"ProcessorFeatures\": \"[]\", \"AutoMinorVersionUpgrade\": \"true\", \"DBSubnetGroupName\": \"default\", \"DeletionProtection\": \"false\", \"DBInstanceIdentifier\": \"cryo-instance-ec2-user-tlrlq1\", \"DBParameterGroupName\": \"default.postgres12\", \"VpcSecurityGroupIds\": \"[[\"sg-3ba6747b\"]]\", \"EnableIAMDatabaseAuthentication\": \"false\", \"CopyTagsToSnapshot\": \"false\", \"PubliclyAccessible\": \"false\", \"MultiAZ\": \"false\", \"Engine\": \"postgres\", \"EnableCloudwatchLogsExports\": \"[]\" }
```

Restaure um cluster do Amazon Aurora

Usar aAWS BackupConsole para restaurar pontos de recuperação do Aurora

AWS Backup restaura o cluster do Aurora; ele não cria nem anexa uma instância do Amazon RDS ao cluster. Nas etapas a seguir, você criará e anexará uma instância do Amazon RDS ao cluster do Aurora restaurado usando a CLI.

Restaurar um cluster do Aurora exige especificar várias opções de restauração. Para obter informações sobre essas opções, consulte [Visão geral do backup e da restauração de um cluster de banco de dados do Amazon Aurora](#) no Amazon Aurora Guia do usuário.

Para restaurar um cluster do Amazon Aurora

1. Abrir oAWS Backupconsole do<https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolhaRecursos protegidosE o ID de recurso do Aurora que você deseja restaurar.
3. Na página Resource details (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 Instance specifications (Especificações de instância), aceite os valores predefinidos ou especifique as opções para as configurações de DB engine (Mecanismo de banco de dados),License Model (Modelo de licença), Capacity type (Tipo de capacidade).

Note

Se o tipo de capacidade Serverless (Sem servidor) estiver selecionado, um painel de Capacity settings (Configurações de capacidade) será exibido. Especifique as opções para as configurações de Minimum Aurora capacity unit (Unidade de capacidade mínima do Aurora) e Maximum Aurora capacity unit (Unidade de capacidade máxima do Aurora) ou escolha opções diferentes na seção Additional scaling configuration (Configuração de dimensionamento adicional).

5. NoConfiguraçõesEspecifique um nome exclusivo para todas as instâncias de cluster de banco de dados pertencentes ao seuAWSNa região da 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. NoRede e segurança, aceite os valores predefinidos ou especifique as opções para oVirtual Private Cloud (VPC),Subnet group, eAvailability zoneConfigurações do .
7. No painel Database options (Opções de banco de dados), aceite os valores predefinidos ou especifique as opções para as configurações de Database port (Porta de banco, de dados), DB cluster parameter group (Group de parâmetros de clusters de banco de dados) e IAM DB Authentication Enabled (Autenticação de banco de dados de IAM habilitada).
8. No painel Backup, aceite o valor predefinido ou especifique a opção para a configuração de Copy tags to snapshots (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 Encryption (Criptografia), aceite os valores predefinidos ou especifique as opções para as configurações de Enable encryption (Habilitar criptografia) ou Disable encryption (Desabilitar criptografia).
11. No painel Log exports (Exportação de logs), escolha os tipos de log a serem publicados no Amazon CloudWatch Logs. A IAM role (Função do IAM) já está definida.

12. No painel de Restore role (Restaurar função), escolha a função 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 é 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 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
```

Usar a AWS Backup API, CLI ou SDK para restaurar pontos de recuperação do Aurora

Use [StartRestoreJob](#). Você pode 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\": \"[]\"}
```

Restaure uma instância do Amazon EC2

Ao usar o console, é possível executar restaurações com 16 opções. Se você precisar definir os outros parâmetros, deverá usar a CLI ou o SDK.

Note

Userdata não é um parâmetro. Ele não é protegido pelo console, pela CLI ou pelo SDK.

Usar o AWS Backup Console para restaurar pontos de recuperação do Amazon EC2

Essa é a opção recomendada.

Para restaurar recursos do Amazon EC2 usando o AWS Backup Console do

1. Abrir o AWS Backup console do <https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolha Recursos protegidos e o ID de recurso do Amazon EC2 que você deseja restaurar.
3. Na página Resource details (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 Network settings (Configurações de rede), aceite os valores predefinidos ou especifique as opções para o Tipo de instância, Virtual Private Cloud (VPC), Subnet (Sub-rede), Grupos de segurança, e Função IAM de instância Configurações do .
5. No Função de restauração, aceite o Função padrão ou Escolha uma função do IAM para especificar a função do IAM que o AWS Backup assumirá para esta restauração.
6. No Configurações avançadas, aceite os valores predefinidos ou especifique as opções para o Comportamento de desligamento, Habilitar a proteção contra encerramento, Placement group, T2/T3 ilimitado, Localização, e Dados do usuário Configurações do . Esta seção é usada para personalizar o comportamento de desligamento e hibernação, proteção contra encerramento, grupos de posicionamento, localização e outras configurações avançadas.
7. Depois de especificar todas as configurações, escolha Restore backup (Restaurar backup).

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

O AWS Backup console permite restaurar pontos de recuperação do Amazon EC2 com os seguintes parâmetros e configurações que você pode personalizar:

- Tipo de instância
- Amazon VPC
- Sub-rede
- Grupos de segurança
- IAM role (Função do IAM)
- Comportamento de desligamento
- Comportamento de parar e hibernar
- Termination protection

- T2/T3 ilimitado
- Nome do placement group
- Instância otimizada para EBS
- Localização
- ID do disco de RAM
- ID do kernel
- Dados do usuário
- Exclusão no término

Esses parâmetros são pré-preenchidos para corresponderem ao backup original. É possível alterá-los antes de restaurar a instância. O AWS Backup identifica parâmetros com valores que podem não ser válidos ou que podem resultar em uma restauração inválida.

Usar aAWS BackupAPI, CLI ou SDK para restaurar pontos de recuperação do Amazon EC2

Use `StartRestoreJob`. Esta opção permite restaurar todos os 38 parâmetros, incluindo os 22 parâmetros que não são personalizáveis no console. O [Referência de API do Amazon EC2](#) lista todos os 38 parâmetros. Isso é adequado se você precisar de todos os 38 parâmetros e estiver confiante com a restauração de parâmetros sem validação. Veja a seguir um exemplo dos metadados que você pode passar para restaurar um ponto de recuperação do Amazon EC2.

```
"restoreMetadata":
{"HibernationOptions":{"configured":false},"InstanceInitiatedShutdownBehavior":"stop","CpuOptions":{"CoreCount":1,"ThreadsPerCore":2},"SubnetId":"subnet-b35676f9","SecurityGroupIds":["sg-09e183a37f21ec0ba"],"EbsOptimized":"false","KeyName":"ec2CanaryKeyPair","DisableApiTermination":"false","VpcId":"vpc-4852ff32","Placement":{"AvailabilityZone":"us-east-1a"},"GroupName":"","Tenancy":"default"},"NetworkInterfaces":[{"AssociatePublicIpAddress":true,"DeleteOnTermination":true,"Description":"","DeviceIndex":0,"Groups":["sg-09e183a37f21ec0ba"],"Ipv6AddressCount":0,"Ipv6Addresses":[],"NetworkInterfaceId":"eni-024f43c22193155e3","PrivateIpAddress":"172.31.24.10","PrivateIpAddresses":[{"Primary":true,"PrivateIpAddress":"172.31.24.10"}],"SecondaryPrivateIpAddressCount":0,"SubnetId":"subnet-b35676f9","InterfaceType":"interface"},"InstanceType":"t3.nano","CapacityReservationSpecification":{"CapacityReservationPreference":"open"},"CreditSpecification":{"CpuCredits":"unlimited"},"Monitoring":{"State":"disabled"}]}
```

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.

Note

AWS Backup usará o key pair SSH usado no momento do backup para executar automaticamente a restauração.

AWS Backup não permite modificar o perfil de instância. Isso é para evitar a possibilidade de encaminhamentos de privilégios. Se você precisar modificar o perfil da instância, faça isso no Amazon EC2.

Para fazer uma restauração com êxito com o perfil de instância original, você deve editar a política de restauração. Se você aplicar um perfil de instância durante a restauração, será necessário atualizar a função de operador e adicionar `PassRole` permissões da função de perfil de instância subjacente para

o Amazon EC2. Caso contrário, o Amazon EC2 não poderá autorizar a inicialização da instância e ela falhará.

Durante uma restauração, todas as cotas e restrições de configuração do Amazon EC2 se aplicam.

Restaurar umaAWS Storage Gatewayvolume

Se você estiver restaurando umAWS Storage GatewaySnapshot de volume, você pode optar por restaurar o snapshot como umAWS Storage GatewayVolume ou como volume do Amazon EBS. Isto é porqueAWS Backupintegra-se com ambos os serviços e qualquerAWS Storage Gatewaypode ser restaurado para umAWS Storage GatewayVolume ou volume do Amazon EBS.

Para restaurar um volume do AWS Storage Gateway

1. Abrir oAWS Backupconsole do<https://console.aws.amazon.com/backup>.
2. No painel de navegação, escolhaRecursos protegidos, em seguida, selecione oAWS Storage GatewayID de recurso que você deseja restaurar.
3. Na página Resource details (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.

para oResource type (Tipo de recurso), escolha a opçãoAWSPara criar ao restaurar esse backup.

5. Se escolherVolume Storage Gateway, escolha umGatewayem um estado acessível. Escolha também o seuNome do destino iSCSI.

1. Para gateways "Volume armazenado", escolha umID de disco.
2. Para gateways "Volume em cache", escolha uma capacidade que seja pelo menos tão grande quanto o seu recurso protegido.

Se você escolher EBS volume (Volume do EBS), forneça os valores para o Volume type (Tipo de volume), Size (GiB) (Tamanho) e escolha uma Availability zone (Zona de disponibilidade).

6. para oFunção de restauração, escolha a função do IAM queAWS Backupassumirá para esta restauração.

Note

Se oAWS BackupA função padrão do não estiver presente na sua conta, umaFunção padrãoO é criado para você com as permissões corretas. Você pode excluir essa função padrão ou torná-la inutilizável.

7. Escolha Restore backup (Restaurar backup).

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

Usar oAWS BackupAPI, CLI ou SDK para restaurar pontos de recuperação do Amazon EC2

Use `StartRestoreJob`.

Gerenciar o AWS Backup recursos em várias AWS contas

É possível usar o recurso de gerenciamento entre contas no AWS Backup para gerenciar e monitorar seus trabalhos de backup, restauração e cópia no AWS que você configura com AWS Organizations. [AWS Organizations](#) O é um serviço que oferece gerenciamento baseado em políticas para várias AWS de uma única conta de gerenciamento. Ele permite que você padronize a maneira como implementa políticas de backup, minimizando erros manuais e esforços simultaneamente. De uma visão centralizada, é possível identificar com facilidade recursos em todas as contas que atendam aos critérios em que você esteja interessado.

Se configurar o AWS Organizations, você poderá configurar o AWS Backup para monitorar atividades em todas as suas contas em um só lugar. Também é possível criar uma política de backup e aplicá-la a contas selecionadas que fazem parte da organização e exibir as atividades de trabalho de backup agregadas diretamente do console do AWS Backup. 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 de gerenciamento.

Por exemplo, você define uma política de backup A que faz backups diários de recursos específicos e os mantém por 7 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 do 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 [Definição de políticas, sintaxe de políticas e herança de políticas](#) (p. 82) no AWS Organizations Guia do usuário do. Para referências adicionais e casos de uso, consulte o blog [Gerenciando backups em escala em seu AWS Organizations usando AWS Backup](#) e o vídeo tutorial [Gerenciando backups em escala em seu AWS Organizations usando AWS Backup](#).

O recurso de gerenciamento entre contas não está disponível no AWS Regiões: AWS GovCloud (US), regiões da China, Oriente Médio (Bahrein) e Ásia-Pacífico (Hong Kong).

Para usar o gerenciamento entre contas, é necessário seguir estas etapas:

1. Crie uma conta de gerenciamento no AWS Organization e adicione contas à conta de gerenciamento.
2. Habilite o recurso de gerenciamento entre contas no AWS Backup.
3. Crie uma política de backup para ser aplicada a todos os AWS em 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-membro.

4. Gerencie trabalhos de backup, restauração e cópia em todos os AWS contas.

Tópicos

- [Criando uma conta de Gerenciamento em Organizations \(p. 78\)](#)
- [Como habilitar o gerenciamento entre contas \(p. 78\)](#)
- [Como criar uma política de backup \(p. 78\)](#)
- [Monitoramento de atividades em váriasAWScontas \(p. 82\)](#)
- [Regras de inclusão de recursos \(p. 82\)](#)
- [Definição de políticas, sintaxe de políticas e herança de políticas \(p. 82\)](#)

Criando uma conta de Gerenciamento em Organizations

Primeiramente, é necessário criar sua organização e configurá-la comAWSContas-membro doAWS Organizations.

Para criar uma conta de gerenciamento noAWS Organizationse adicionar contas

- Para obter instruções, consulte[Tutorial: Criar e configurar uma organização](#)noAWS OrganizationsGuia do usuário do.

Como habilitar o gerenciamento entre contas

Antes que possa usar o gerenciamento entre contas no AWS Backup, é necessário habilitar o recurso (ou seja, incluí-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. Faça login noAWS Management Consolee abra oAWS Backupconsole do em<https://console.aws.amazon.com/backup>.

Isso só pode ser feito pela 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 de várias 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.

Como criar uma política de backup

Depois de habilitar o gerenciamento entre contas, crie uma política de backup entre contas pela conta de gerenciamento.

Para criar uma política de backup

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.
 - 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 da 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.

Verifique se o cofre de backup existe 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 outro AWS Região 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. No Atribuição de recursos, forneça o nome da AWS Identity and Access Management Função do (IAM) do. Para usar a AWS Backup Função vinculada ao serviço do serviço, forneça `service-role/AWSBackupDefaultServiceRole`.

AWS Backup assume essa função em cada conta para obter as permissões para executar trabalhos de backup e cópia, incluindo permissões de chave de criptografia quando aplicável. AWS Backup também usa essa função para executar exclusões do ciclo de vida.

Note

O AWS Backup não valida se a função existe ou se a função pode ser assumida. Planos de backup criados pelo gerenciamento entre contas, AWS Backup usará as configurações de inclusão da conta de gerenciamento e substituirá as contas específicas das configurações.

Para cada conta à qual você deseja adicionar políticas de backup, é necessário criar os cofres e as funções do IAM por conta própria.

9. Adicione tags ao plano de backup se desejar.
10. No Configurações avançadas Seção, selecione VSS do Windows se o recurso que você está fazendo backup estiver executando o Microsoft Windows em uma instância do Amazon EC2. Isso permite que você faça backups do Windows VSS consistentes com aplicativos.

Note

AWS Backup atualmente suporta backups consistentes com aplicativos de recursos em execução somente no Amazon EC2. Nem todos os tipos de instância ou aplicativos são suportados para backups do Windows VSS. Para obter mais informações, consulte [Criando backups do Windows VSS \(p. 47\)](#).

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 um exemplo a seguir: AWS Política das Organizations que cria um plano de backup. Se você habilitar Backup do Windows VSS, você precisa adicionar permissões que permitam fazer backups consistentes com aplicativos Como mostrado no `advanced_backup_settings` seção da política.

```
{
  "plans": {
    "PiiMasterBackupPlan": {
      "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": "2"
            },
            "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": "28"
                },
                "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"
        ]
      }
    },
    "advanced_backup_settings": {
      "ec2": {
        "windows_vss": {
          "@@assign": "enabled"
        }
      },
      "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 sua 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. No momento, o AWS Backup não fornece validação de política para o AWS Organizations SDK e JSON.

Se as políticas aplicadas à conta de gerenciamento e a uma conta de membro conflito, ambas as políticas serão executadas sem problemas (ou seja, as políticas serão executadas independentemente para cada conta). Por exemplo, se a política mestre 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 entre diferentes políticas), o AWS Backup não aplica a política à conta. Se algumas configurações não forem válidas, o AWS Backup as ajusta.

Independentemente das configurações de inclusão em uma conta de membro em um plano de backup criado a partir de uma política de backup, o AWS Backup usará as configurações de opt-in 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.

Monitoramento de atividades em várias AWS contas

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 [Como habilitar o gerenciamento entre contas](#) (p. 78).

Como monitorar várias contas

1. Faça login no AWS Management Console e abra o AWS Backup console do em <https://console.aws.amazon.com/backup>.

Isso só pode ser feito pela 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 AWSID da conta e você 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 no nível da organização (com um ID iniciando `orgs-`), o AWS Backup configurações de ativação para a conta de gerenciamento de Organizations substituirão as configurações de aceitação nessa conta de membro, mas somente para esse plano de backup.

Se a conta de membro também tiver planos de backup de nível local criados por usuários, esses planos de backup seguirão as configurações de ativação na conta de membro, sem referência às configurações de ativação da conta de gerenciamento de Organizations.

Definição de políticas, sintaxe de políticas e herança de políticas

Os tópicos a seguir estão documentados no Guia do usuário do Organizations.

- Políticas de backup— Consulte [Políticas de backup](#).
- Sintaxe da política— Consulte [Sintaxe e exemplos de políticas de backup](#).
- Herança para tipos de política de gerenciamento— Consulte [Herança para tipos de política de gerenciamento](#).

O uso do AWS CloudFormation Modelos com AWS Backup

Em geral

com AWS CloudFormation, você pode provisionar e gerenciar seus recursos do de forma segura e repetível usando modelos criados por você. Você pode usar modelos do AWS CloudFormation 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 AWS CloudFormation Trabalho?](#) no AWS CloudFormation Guia do usuário do.

Antes de criar sua pilha do AWS CloudFormation, você deve considerar o seguinte:

- Recomendamos criar modelos separados para seus planos de backup e seus cofres de backup. Como os cofres de backup só podem ser excluídos se estiverem vazios, você não poderá excluir uma pilha que inclua cofres de backup se eles contiverem pontos de recuperação.
- Antes de criar a pilha, certifique-se de que tem uma função de serviço disponível. A função de serviço padrão do AWS Backup é criada para você na primeira vez que atribuir recursos a um plano de backup. Se você ainda não tiver feito isso, a função de serviço padrão não estará disponível. Você também pode especificar uma função personalizada que criar. Para obter mais informações sobre funções do , consulte [Funções de serviço IAM \(p. 103\)](#).

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

```
Description: Backup Plan template to back up all resources tagged with backup=daily 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"
      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
```

Note

Se você estiver usando a função de serviço padrão, substitua *Função de serviço* por `AWSBackupServiceRolePolicyForBackup`.

Com o Windows VSS

```
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
```

Para obter informações sobre como usar o AWS CloudFormation para o AWS Backup, consulte [AWS Backup Referência do tipo de recurso](#) no AWS CloudFormation Guia do usuário do.

Para obter informações sobre como controlar o acesso aos recursos de serviço ao usar o AWS CloudFormation, consulte [Como controlar o acesso com o AWS Identity and Access Management](#) no AWS CloudFormation Guia do usuário do.

O uso do AWS CloudFormation Com Organizations

Você pode [usar o AWS CloudFormation StackSets](#) em várias contas em uma [AWS Organização](#). Modelos de exemplo estão disponíveis no [AWS CloudFormation Guia do usuário do](#).

Use o seguinte YAML do AWS CloudFormation modelo e função do Lambda para implantar o AWS Backup políticas no nível Organizations. O YAML implanta o AWS Backup políticas no nível organization. A função do Lambda (em Python) é referenciada pelo YAML e implanta o AWS CloudFormation Template

```
AWSTemplateFormatVersion: '2010-09-09'
Description: This template deploys backup policies required to manage backups at an
organization level.

Parameters:
  ImpactedAccounts:
    Description: "CSV list of the Org Ids"
    Type: CommaDelimitedList
    Default: ""

  ConfigBucket:
    Description: S3 Bucket for the Custom Lambda Code and Templates
    Type: String
    Default: mb3-venkitas

  ConfigBucketKey:
    Description: S3 Key for the Custom Lambda Code and Templates
    Type: String
    Default: IaC/cfn-templates/Backup/

Resources:
  #Type='SERVICE_CONTROL_POLICY'|'TAG_POLICY'|'BACKUP_POLICY'|'AISERVICES_OPT_OUT_POLICY'
  GoldDailyBackupPolicySyd:
    Type: Custom::OrgPolicy
    Properties:
      PolicyName: GoldDailyBackupPolicySyd
      PolicyType: BACKUP_POLICY
      PolicyTargets : !Ref ImpactedAccounts
      PolicyDescription: >-
        BackupPolicy for Daily Backup as per the resource selection criteria
      PolicyContents: |-
        {
          "plans": {
            "OrgDailyBackupPlan": {
              "regions": {
                "@@assign": [
                  "REGION"
                ]
              },
              "rules": {
                "OrgDailyBackupRule": {
                  "schedule_expression": {
                    "@@assign": "SCHEDULE_EXPRESSION"
                  },
                  "start_backup_window_minutes": {
                    "@@assign": "480"
                  },
                  "complete_backup_window_minutes": {
                    "@@assign": "720"
                  },
                  "lifecycle": {
                    "delete_after_days": {
                      "@@assign": "1"
                    }
                  },
                  "target_backup_vault_name": {
                    "@@assign": "DailyBackupVault"
                  },
                  "recovery_point_tags": {
                    "project": {
                      "tag_key": {
                        "@@assign": "TAG_KEY"
                      },
                      "tag_value": {
                        "@@assign": "TAG_VALUE"
                      }
                    }
                  }
                }
              }
            }
          }
        }
```

```
    }
  },
  "backup_plan_tags": {
    "project": {
      "tag_key": {
        "@@assign": "TAG_KEY"
      },
      "tag_value": {
        "@@assign": "TAG_VALUE"
      }
    }
  },
  "selections": {
    "tags": {
      "OrgDailyBackupSelection": {
        "iam_role_arn": {
          "@@assign": "arn:aws:iam::$account:role/BackupRole"
        },
        "tag_key": {
          "@@assign": "TAG_KEY"
        },
        "tag_value": {
          "@@assign": [
            "TAG_VALUE"
          ]
        }
      }
    }
  }
}

Variables:
- REGION : !Ref 'AWS::Region'
- TAG_KEY : project
- TAG_VALUE : aws-backup-demo
- SCHEDULE_EXPRESSION : "cron(0 5 ? * * *)"
ServiceToken: !GetAtt OrgPolicyCustomResourceManager.Arn

DenyVaultAndLogBucketOperationsSCP:
  Type: Custom::OrgPolicy
  Properties:
    PolicyName: SCP_DENY_VAULT_AND_LOG_BUCKET_OPERATIONS
    PolicyType: SERVICE_CONTROL_POLICY
    PolicyTargets : !Ref ImpactedAccounts
    PolicyDescription: >-
      This SCP denies operations on Vault and log bucket that are tagged with a specific
      project name.
    PolicyContents: |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Sid": "DenyLogBucketOperations",
            "Effect": "Deny",
            "Action": [
              "s3:DeleteBucket",
              "s3:DeleteBucketPolicy",
              "s3:DeleteJobTagging",
              "s3:DeleteAccessPointPolicy",
              "s3:DeleteAccessPoint",
              "s3:DeleteBucketWebsite"
            ],
            "Resource": [
```

```
        "arn:aws:s3:::LOG_BUCKET-*"
      ],
    },
    {
      "Sid": "DenyLogBucketObjectOperations",
      "Effect": "Deny",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::LOG_BUCKET-*/*"
      ]
    },
    {
      "Sid": "DenyVaultOperations",
      "Effect": "Deny",
      "Action": [
        "backup:DeleteBackupVault",
        "backup:DeleteBackupSelection",
        "backup:DeleteBackupPlan",
        "backup:DeleteBackupVaultAccessPolicy",
        "backup:DeleteBackupVaultNotifications",
        "backup:DeleteRecoveryPoint",
        "backup:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/TAG_KEY": [
            "TAG_VALUE"
          ]
        }
      }
    }
  ]
}

Variables:
  - REGION : !Ref 'AWS::Region'
  - LOG_BUCKET : backup-log-bucket
  - TAG_KEY : project
  - TAG_VALUE : aws-backup-demo
ServiceToken: !GetAtt OrgPolicyCustomResourceManager.Arn

OrgPolicyCustomResourceManager:
  Type: AWS::Lambda::Function
  Properties:
    FunctionName: OrgPolicyCustomResourceManager
    Description: Lambda function to deploy CloudFormation custom resources
                  for Organization SCPs.
    Handler: OrgPolicyCustomResourceManager.lambda_handler
    Code:
      S3Bucket: !Ref ConfigBucket
      S3Key: !Sub
        - '${S3Prefix}OrgPolicyCustomResourceManager.zip'
        - { S3Prefix: !Ref ConfigBucketKey }
    Role: !GetAtt OrgPolicyCustomResourceManagerRole.Arn
    Runtime: python3.7
    MemorySize: 256
    Timeout: 300
    Tags:
      - Key: Name
```

```
Value: OrgPolicyCustomResourceManager

OrgPolicyCustomResourceManagerRole:
  Type: 'AWS::IAM::Role'
  Properties:
    AssumeRolePolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Principal:
            Service: 'lambda.amazonaws.com'
          Action:
            - 'sts:AssumeRole'
    Path: '/'
    ManagedPolicyArns:
      - 'arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole'
    Policies:
      - PolicyName: AssumeOrgRole
        PolicyDocument:
          Statement:
            - Effect: Allow
              Action:
                - sts:AssumeRole
              Resource: '*'
      - PolicyName: OrgPermissions
        PolicyDocument:
          Statement:
            - Effect: Allow
              Action:
                - organizations:CreatePolicy
                - organizations>DeletePolicy
                - organizations:AttachPolicy
                - organizations:DetachPolicy
                - organizations:ListPolicies
              Resource: '*'
      - PolicyName: S3Permissions
        PolicyDocument:
          Statement:
            - Effect: Allow
              Action:
                - s3:Get*
              Resource:
                !Sub
                - 'arn:aws:s3:::${Bucket}/*'
                - { Bucket: !Ref ConfigBucket }
```

```
import boto3
#https://pypi.org/project/cfnresponse/
import cfnresponse as cfn
import logging
import uuid

logger = logging.getLogger()
logger.setLevel(logging.INFO)
client = boto3.client('organizations')

def get_policy(event):
    policy_contents = ''
    if 'PolicyContents' in event['ResourceProperties']:
        policy_contents = event['ResourceProperties']['PolicyContents']
    else:
        s3_bucket = event['ResourceProperties']['PolicyBucket']
        s3_object = event['ResourceProperties']['PolicyLocation']
        s3 = boto3.resource('s3')
```



```
policy_file = s3.Object(s3_bucket, s3_object)
policy_contents = policy_file.get()['Body'].read().decode('utf-8')

#Check for replacement variables
if 'Variables' in event['ResourceProperties']:
    variables= event['ResourceProperties']['Variables']
    logger.info(f"variables : {variables}")
    for variable in variables:
        for key, value in variable.items():
            logger.info(f"Replacing Key : {key} with value : {value}")
            policy_contents = policy_contents.replace(key,value )

return policy_contents

def lambda_handler(event, context):
    try:
        #create physical resource id
        customResourcePhysicalID = uuid.uuid4().hex

        if 'PhysicalResourceId' in event:
            customResourcePhysicalID = event['PhysicalResourceId']

        logger.info(f"OrgPolicyCustomResourceManager Request: {event}")
        resource_action = event['RequestType']
        policy_name = event['ResourceProperties']['PolicyName']
        policy_contents = get_policy(event)
        policy_type = event['ResourceProperties']['PolicyType']
        policy_description = event['ResourceProperties']['PolicyDescription']

        policyTargetList=[]
        if 'PolicyTargets' in event['ResourceProperties']:
            policy_targets = event['ResourceProperties']['PolicyTargets']
            policyTargetList = policy_targets

        logger.info(f"policy_targets: {policy_targets}")

        if resource_action == 'Create':
            logger.info(f"Action : {resource_action} policy")
            response = client.create_policy(
                Content=policy_contents,
                Description=policy_description,
                Name=policy_name,
                Type=policy_type
            )
            logger.info(f"Response: {response}")
            policyId = response['Policy']['PolicySummary']['Id']
            #Attach the policy in target accounts
            for policyTarget in policyTargetList:
                try:
                    logger.info(f"Attaching {policyId} on Account {policyTarget}")
                    response = client.attach_policy(PolicyId=policyId,
                                                    TargetId=policyTarget)

                    logger.info(f"Attached {policyId} on Account {policyTarget}")

                except Exception as e:
                    logger.error(str(e))

            cfn.send(event, context, cfn.SUCCESS,
                    {'Message': "Policy created successfully."}, customResourcePhysicalID)

        elif resource_action == 'Update' or resource_action == 'Delete':
            logger.info(f" Action: {resource_action} policy, policy_type: {policy_type},
            policy_name {policy_name}")
            response = client.list_policies(Filter=policy_type)
```

```
        policy = list(filter(lambda item: item['Name'] == policy_name,
response["Policies"]))
        logger.info(f"Policy Found : {policy}")

        if len(policy) == 0:
            return {'Status': 'Policy not found for name ' + policy_name}

        policyId=policy[0]['Id']
        if resource_action == 'Delete':
            #Detach the policy
            detachPolicy(policyTargetList,policyId)

            while True:
                try:
                    response = client.delete_policy(PolicyId=policyId)
                    logger.info(f"deletePolicy response: {response}")
                    cfn.send(event, context, cfn.SUCCESS,
                        {'Message': "Policy modified successfully."},
customResourcePhysicalID)
                    break
                except client.exceptions.PolicyInUseException as e:
                    #try detaching the policy again
                    detachPolicy(policyTargetList,policyId)
                    logger.error(str(e))

            else:
                response = updatePolicy(resource_action,policyId, policy_contents)
                logger.info(f"updatePolicy response: {response}")
                cfn.send(event, context, cfn.SUCCESS,
                    {'Message': "Policy modified successfully."}, customResourcePhysicalID)

        else:
            logger.error(f"Unexpected Action : {resource_action}")
            cfn.send(event, context, cfn.FAILED,
                {'Message': 'Unexpected event received from CloudFormation'},
                customResourcePhysicalID)
    except Exception as exc:
        logger.error(f"Exception: {str(exc)}")
        cfn.send(event, context, cfn.FAILED,
            {'Message': str(exc)}, customResourcePhysicalID)

def detachPolicy(policyTargetList,policyId):
    #Detach the policy in target accounts
    for policyTarget in policyTargetList:
        try:
            logger.info(f"Detaching {policyId} from Account {policyTarget}")
            response = client.detach_policy(PolicyId=policyId,
                TargetId=policyTarget)

            logger.info(f"Detached {policyId} from Account {policyTarget}")
        except Exception as e:
            logger.error(str(e))

def updatePolicy(resource_action, policyId, policy_contents):
    logger.info(f"updatePolicy with action : {resource_action}, policyId : {policyId}")
    if (resource_action == 'Update'):
        response = client.update_policy(
            PolicyId=policyId,
            Content=policy_contents
        )
    return response
```

Segurança em AWS Backup

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isto como segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem** — A AWS é responsável por proteger a infraestrutura que executa os serviços da AWS na nuvem da AWS. A 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 [programas de conformidade da AWS](#). Para saber mais sobre os programas de conformidade que se aplicam ao AWS Backup, consulte [Serviços da AWS no escopo pelo programa de conformidade](#).
- **Segurança da nuvem: sua responsabilidade** é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AWS Backup. Os tópicos a seguir mostram como configurar o AWS Backup para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros serviços da AWS que ajudam a monitorar e proteger os recursos do AWS Backup.

Tópicos

- [Proteção de dados no AWS Backup](#) (p. 93)
- [Identity and Access Management no AWS Backup](#) (p. 97)
- [Validação de conformidade do AWS Backup](#) (p. 165)
- [Resiliência no AWS Backup](#) (p. 166)
- [Segurança da infraestrutura no AWS Backup](#) (p. 167)

Proteção de dados no AWS Backup

AWS Backup está em conformidade com o [AWS Modelo de responsabilidade compartilhada](#) (Opcional), que inclui regulamentos e diretrizes para proteção de dados. A AWS é responsável pela proteção da infraestrutura global que executa todos os serviços da AWS. A AWS mantém o controle sobre os dados hospedados nessa infraestrutura, incluindo os controles de configuração de segurança para lidar com conteúdos e dados pessoais dos clientes. Os clientes e os parceiros da Partner Network (APN), atuando como controladores de dados ou processadores de dados, são responsáveis por todos os dados pessoais que colocam na AWS Nuvem.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da conta da AWS e configure as contas de usuário individuais com o AWS Identity and Access Management. 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 as soluções de criptografia da AWS com todos os controles de segurança padrão nos produtos da AWS.

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 Name (Nome). Isso também vale para o uso do AWS Backup ou de outros serviços da AWS com o console, a API, a AWS CLI ou os AWS SDKs. 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 obter 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 noAWS

A maneira de configurar a criptografia difere de acordo com o tipo de recurso. Certos tipos de recursos são compatíveis com a capacidade de criptografar seus backups usando uma chave de criptografia diferente da chave usada para criptografar o recurso de origem. Esse recurso adiciona outra camada de proteção para seus backups.

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.

Tipo de recurso	Como configurar criptografia	Criptografia de backup independente
Amazon Elastic File System (Amazon EFS)	Os backups do Amazon EFS são sempre criptografados. O AWS KMS chave de criptografia para backups do Amazon EFS é configurada no AWS Backup no qual os backups do Amazon EFS são armazenados.	Compatível
Amazon Elastic Block Store (Amazon EBS)	Os snapshots do Amazon EBS são criptografados automaticamente com a mesma chave de criptografia que foi usada para criptografar o volume do EBS de origem. Os snapshots de volumes do EBS não criptografados também não são criptografados.	Não suportado
AMIs do Amazon Elastic Compute Cloud (Amazon EC2)	As AMIs do Amazon EC2 compatíveis com snapshots do Amazon EBS são criptografadas automaticamente com a mesma chave de criptografia que foi usada para criptografar o volume do EBS de origem. Os snapshots das AMIs do não criptografadas também não são criptografados.	Não suportado
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 do Amazon RDS de	Não suportado

Tipo de recurso	Como configurar criptografia	Criptografia de backup independente
	<p>origem. Os snapshots de bancos de dados do Amazon RDS do não criptografados também não são criptografados.</p> <p>Note</p> <p>AWS Backup é compatível com todos os mecanismos de banco de dados do Amazon RDS, inclusive o Amazon Aurora</p>	
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 do Aurora do não criptografados também não são criptografados.	Não suportado
Amazon DynamoDB	<p>Os backups do DynamoDB são criptografados automaticamente com a mesma chave de criptografia que foi usada para criptografar a tabela do DynamoDB de origem. Os snapshots das tabelas do DynamoDB do não criptografados também não são criptografados.</p> <p>Note</p> <p>Em ordem para AWS Backup para criar um backup de uma tabela criptografada do DynamoDB, você deve adicionar as permissões <code>kms:Decrypt</code> e <code>kms:GenerateDataKey</code> para a função do IAM usada para o backup. Como alternativa, você pode usar a AWS Backup Função de serviço padrão.</p>	Não suportado

Tipo de recurso	Como configurar criptografia	Criptografia de backup independente
AWS Storage Gateway	<p>Os snapshots do AWS Storage Gateway são criptografados automaticamente com a mesma chave de criptografia que foi usada para criptografar o volume do AWS Storage Gateway de origem. Os snapshots de volumes do AWS Storage Gateway não criptografados também não são criptografados.</p> <p>Note</p> <p>Não é necessário usar uma chave gerenciada pelo cliente em todos os serviços para habilitar oAWS Storage Gateway. Você só precisa 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 gerenciada do AWS KMS específica do serviço.</p>	Não suportado
Amazon FSx	<p>Os recursos de criptografia para sistemas de arquivos do Amazon FSx diferem com base no sistema de arquivos subjacente. Para saber mais sobre seu sistema de arquivos específico do Amazon FSx, consulte oGuia do usuário do FSx.</p>	Não suportado

Criptografia para cópias de backup

O AWS Backup criptografa cópias de backup por padrão sempre que possível, mesmo que o backup original não esteja criptografado.

Você tem duas opções para criptografar cópias de backup:

1. Use a padrãoAWSChave KMS para o cofre de backup de destino. A chave padrão é diferente para cada serviço e é gerenciada pela AWS.
2. Designe uma chave gerenciada pelo cliente através do cofre de destino. Essa é a única opção compatível para backups do AWS Storage Gateway.

Privilégio mínimo

O exemplo de política a seguir ilustra a menor quantidade de privilégio em uma política de chave do KMS para copiar um snapshot criptografado do Amazon RDS do AWS GovCloud (EUA-Leste) (conta 1122*) para o AWS GovCloud (EUA-Oeste) (conta 9988*, com a chave lá).

```
{
  "Sid": "Allow use of the key - added",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws-us-gov:iam::112233445566:root"
  },
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": [
        "rds.us-gov-west-1.amazonaws.com",
        "backup.us-gov-west-1.amazonaws.com"
      ],
      "kms:CallerAccount": "998877665544"
    }
  }
}
```

Para obter mais informações sobre AWS KMS, consulte [O que é o AWS KMS?](#)

Para saber mais sobre criptografia de backup de cada serviço com o qual o AWS Backup é compatível, consulte os seguintes links:

- [Como criptografar seus dados usando o AWS Key Management Service](#) no AWS Storage Gateway Guia do usuário do.
- [Criptografia de recursos do Amazon RDS](#) no Guia do usuário do Amazon RDS

Identity and Access Management no AWS Backup

O acesso ao AWS Backup requer credenciais. Essas credenciais devem ter permissões para acessar o AWS, como um banco de dados do Amazon DynamoDB ou um volume do Amazon EBS. As seguintes seções fornecem detalhes. [AWS Identity and Access Management \(IAM\)](#) e [AWS Backup](#) Para ajudar a proteger o acesso a seus recursos.

Warning

Se você excluir credenciais do IAM usadas pelo AWS Backup, ele não pode gerenciar seus backups. Isso é válido mesmo se você criar novas credenciais do IAM posteriormente com as mesmas permissões.

Tópicos

- [Authentication](#) (p. 98)
- [Controle de acesso](#) (p. 99)
- [Funções de serviço IAM](#) (p. 103)
- [Políticas gerenciadas para o AWS Backup](#) (p. 104)

- [Funções vinculadas ao serviço para oAWS Backup \(p. 160\)](#)
- [Atualizações de políticas doAWS Backup \(p. 162\)](#)

Authentication

Acesso aoAWS Backupou oAWSOs serviços dos quais você está fazendo backup exigem credenciais que oAWSO pode usar para autenticar suas solicitações. Você pode acessar a AWS como alguns dos seguintes tipos de identidade:

- **AWSUsuário raiz de conta da—** Quando você cadastrar-se noAWS(Opcional), você fornece um endereço de e-mail e uma senha que é associada aoAWSconta. Esse será seu usuário raiz da conta da AWS. As credenciais fornecem acesso total a todos os recursos da AWS.

Important

Por motivos de segurança, recomendamos usar o usuário-raiz apenas para criar um administrador. O administrador é umUsuário do IAMcom permissões completas para o seuAWSconta. Em seguida, use esse usuário administrador para criar outros usuários e funções do IAM com permissões limitadas. Para obter mais informações, consulte[Práticas recomendadas do IAMeCriação do primeiro grupo e usuário administrador do IAM](#)noIAM User Guide.

- **Usuário do IAM— Um**[Usuário do IAM](#)**é uma identidade dentro do seuAWSConta do que tem permissões personalizadas específicas (por exemplo, permissões para criar um cofre de backup no qual seus backups serão armazenados). Você pode usar uma senha e um nome do usuário do IAM para fazer login em páginas da Web seguras da AWS como [AWS Management Console](#), [Fóruns de discussão da AWS](#) ou a [Central de AWS Support](#).**

Além de um nome e senha de usuário, você também pode gerar [chaves de acesso](#) para cada usuário. Você pode usar essas chaves ao acessar oAWSServiços de forma programática, seja através deum [dos vários SDKs](#)ou usando o[AWS Command Line Interface\(AWSCLI\)](#). 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 autenticação de solicitações, consulte[Processo de assinatura do Signature versão 4](#)noAWSReferência geral.

- **IAM role (Função do IAM)— Um**[IAM role \(Função do IAM\)](#)**é outra identidade do IAM que você pode criar em sua conta que tem permissões específicas. É semelhante a um usuário do IAM, mas não está associada a uma pessoa específica. Uma função do IAM permite obter chaves de acesso temporárias que podem ser usadas para acessarAWSServiços e recursos do. As funções do IAM com credenciais temporárias são úteis nas seguintes situações:**
 - **Acesso de usuário federado:** em vez de criar um usuário do IAM, você poderá usar identidades de usuário já existentes noAWS Directory Service, o diretório de usuário da sua empresa ou um provedor de identidades da web. Estes 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 Guia do usuário do IAM.
 - **Administração entre contas —** você pode usar uma função do IAM em sua conta para conceder outraAWSpara administrar os recursos da sua conta. Para ver um exemplo, consulte[Tutorial: Delegar acesso entre osAWSContas usando funções do IAM](#)noIAM User Guide.
 - **AWSAcesso de serviço —** Você pode usar uma função do IAM em sua conta para conceder umaAWSAs permissões de serviço do para acessar os recursos da sua conta. Para obter mais informações, consulte[Criação de uma função para delegar permissões a umAWSServiço](#)noIAM User Guide.
 - **Aplicações em execução no Amazon Elastic Compute Cloud (Amazon EC2):** é possível usar uma função do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do Amazon EC2 e fazerAWSSolicitações de API. É preferível fazer isso do que armazenar

chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, crie um perfil de instância que esteja 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 uma função 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 as solicitações, mas, a menos que tenha as permissões adequadas, não poderá acessar os recursos do AWS Backup, como os cofres de backup. Também não será possível fazer backup do AWS Recursos como volumes do Amazon Elastic Block Store (Amazon EBS).

Cada recurso da AWS é de propriedade de uma conta da AWS, e as permissões para criar ou acessar um recurso são regidas por políticas de permissões. Um administrador de conta pode associar políticas de permissões ao 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 [Melhores práticas do 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 \(p. 99\)](#)
- [Propriedade do recurso \(p. 100\)](#)
- [Especificar os elementos da política: ações, efeitos e principais \(p. 100\)](#)
- [Especificar condições em uma política \(p. 101\)](#)
- [Permissões da API do: referência de ações, recursos e condições \(p. 101\)](#)
- [Copiar tags permissões \(p. 101\)](#)
- [Políticas de acesso \(p. 102\)](#)

Recursos e operações

Um recurso é um objeto que existe dentro de um serviço. Os recursos do AWS Backup incluem planos de backup, cofres de backup e backups. O termo Backup se refere, de forma geral, a vários tipos de recursos de backup existentes na AWS. Por exemplo, snapshots do Amazon EBS, snapshots do Amazon Relational Database Service (Amazon RDS) e backups do Amazon DynamoDB são tipos de recursos de backup.

No AWS Backup, os backups também são chamados de pontos de recuperação. Ao usar o AWS Backup, você também trabalha com os recursos de outros AWS Serviços que você 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 exclusivamente os recursos da AWS. Você deve ter um ARN quando precisar especificar um recurso sem ambiguidade em todas as AWS, como em políticas do IAM ou chamadas de API.

A tabela a seguir lista recursos, sub-recursos e formatos de ARN.

AWS Backup ARNs do recurso

Tipo de recurso	Formato de Nome de região da Amazon (ARN)
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 do Amazon EBS	arn:aws:ec2:region::snapshot/*
Ponto de recuperação do Amazon EFS	arn:aws:backup:region:account-id:recovery-point:*
Ponto de recuperação do Amazon RDS	arn:aws:rds:region:account-id:snapshot:awsbackup:*
Ponto de recuperação do Amazon Aurora	arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*
Ponto de recuperação para o AWS Storage Gateway	arn:aws:ec2:region::snapshot/*
Ponto de recuperação do DynamoDB	arn:aws:dynamodb:region:account-id::table/*/backup/*

O AWS Backup fornece um conjunto de operações para trabalhar com recursos do AWS Backup. Para obter uma lista das operações disponíveis, consulte [AWS Backup Actions \(p. 207\)](#).

Propriedade do recurso

A conta da AWS possui os recursos criados na conta, independentemente de quem os criou. Especificamente, o proprietário do recurso é o AWS conta do [entidade principal](#) (isto é, o AWS Usuário raiz da conta do, um usuário do IAM ou uma função do IAM) que autentica a solicitação de criação do recurso. Os exemplos a seguir ilustram como isso funciona:

- Se você usar o AWS Credenciais do usuário raiz da conta da AWS Para criar um cofre de backup, o AWS conta é o proprietário do cofre.
- Se você criar um usuário do IAM no seu AWS Se conceda permissões para criar um cofre de backup a esse usuário, o usuário poderá criar um cofre de backup. No entanto, seu AWS Conta da à qual o usuário pertence é a proprietária do recurso do cofre de backup.
- Se você criar uma função do IAM no seu AWS Com permissões para criar um cofre de backup, qualquer pessoa que possa assumir a função poderá criar um cofre do. Suas AWS Conta da à qual a função pertence é a proprietária do recurso do cofre de backup.

Especificar os elementos da política: ações, efeitos e principais

Para cada recurso do AWS Backup (consulte [Recursos e operações \(p. 99\)](#)), o serviço define um conjunto de operações de API (consulte [Actions \(p. 207\)](#)). Para conceder permissões a essas operações da API, o AWS Backup define um conjunto de ações que podem ser especificadas 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 Amazon Resource Name (ARN – Nome de recurso da Amazon) para identificar o recurso a que a política se aplica. Para obter mais informações, consulte [Recursos e operações \(p. 99\)](#).

- **Ação:** você usa palavras-chave de ação para identificar operações de recursos que você 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, o que pode fazer para ter a certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso.
- **Principal:** em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é implicitamente o principal. Para as políticas baseadas em recursos, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam permissões (aplica-se somente a políticas baseadas em recursos).

Para saber mais sobre a sintaxe da política do IAM e as descrições, consulte [Referência de políticas JSON IAM](#) no IAM User Guide.

Para obter uma tabela que mostra todas as ações de API do AWS Backup, consulte [Permissões da API do: referência de ações, recursos e condições](#) (p. 101).

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, convém que uma política só seja aplicada após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política, consulte [Condição](#) no Guia do usuário do IAM.

Para expressar condições, você usa chaves de condição predefinidas. Não existem chaves de condição específicas do AWS Backup. No entanto, existem chaves de condição em toda a AWS que você pode usar conforme apropriado. Para obter uma lista completa de AWS-teclas largas, consulte [AWSChaves de contexto de condição da globais](#) no IAM User Guide.

Note

O AWS Backup não é compatível com condições de chave de contexto ou tags em políticas de acesso para qualquer uma de suas ações.

Permissões da API do: referência de ações, recursos e condições

Ao configurar [Controle de acesso](#) (p. 99) e escrever uma política de permissões que pode anexar a uma identidade do IAM (políticas com base em identidade), você pode usar a em lista como referência. O A lista inclui Cada AWS Backup Operação da API do, as ações correspondentes para as quais você pode conceder permissões para executar a ação e a função AWS 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.

Você pode usar as chaves de condição usadas por toda a AWS em suas políticas do AWS Backup para expressar condições. Para obter uma lista completa das chaves da AWS, consulte [Chaves disponíveis](#) no Guia do usuário do IAM.

Copiar tags permissões

Quando AWS Backup executa um trabalho de backup ou cópia, ele tenta copiar as tags do recurso de origem (ou ponto de recuperação, no caso de cópia) para o ponto de recuperação.

Note

AWS Backup não copia tags durante os trabalhos de restauração.

Durante um trabalho de cópia de segurança ou cópia, AWS Backup agrega as tags especificadas no plano de backup (ou backup sob demanda) com as tags do recurso de origem. Se AWS Backup não pode copiar

todas as tags para o ponto de recuperação, ele falhará no trabalho. Isso pode acontecer pelos seguintes motivos:

- Seu recurso tem mais de 50 tags depois de agregar suas tags de trabalho de backup com suas tags de recurso de origem. AWS oferece suporte a até 50 tags por recurso. Para obter mais informações, consulte [Limites de tag](#) no AWS Guia de referência geral do.
- A função do IAM que você fornece para 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 funções do IAM, consulte [políticas gerenciadas pela](#).

Você pode usar seu plano de backup para criar tags que contradizem suas tags de recurso de origem. Quando os dois entram em conflito, as tags do seu plano de backup têm precedência. Use essa técnica se preferir não copiar um valor de tag do recurso de origem. Especifique a mesma chave de tag, mas um valor diferente ou vazio, usando seu plano de backup.

Permissões necessárias para atribuir tags a backups

Tipo de recurso	Permissão obrigatória
Sistema de arquivos do Amazon EFS	<code>elasticfilesystem:DescribeTags</code>
Sistema de arquivos do Amazon FSx	<code>fsx:ListTagsForResource</code>
Banco de dados do Amazon RDS e cluster do Amazon Aurora	<code>rds:AddTagsToResource</code> <code>rds:ListTagsForResource</code>
Volume do AWS Storage Gateway	<code>storagegateway:ListTagsForResource</code>
Volume da instância do Amazon EC2 e do Amazon EBS	<code>EC2:CreateTags</code> <code>EC2:DescribeTags</code>

O DynamoDB não é compatível com a atribuição de tags a backups. AWS Backup não copia tags de tabelas.

Quando um backup do Amazon EC2 cria um ponto de recuperação de imagem e um conjunto de snapshots, AWS Backup copia tags para a AMI do 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 conhecidas como políticas baseadas em recursos. O AWS Backup é compatível com políticas baseadas em identidade e em recursos.

Note

Esta seção discute o uso do IAM no contexto do 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 IAM User Guide. Para obter mais informações sobre a sintaxe e da política do IAM, consulte [Referência de políticas JSON IAM](#) no IAM User Guide.

Políticas baseadas em identidade (políticas do IAM)

As políticas baseadas em identidade são políticas que você pode anexar 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 recursos, mas impede que eles restaurem 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 usar as políticas do IAM para controlar o acesso a backups, consulte [Políticas gerenciadas \(p. 104\)](#).

Políticas baseadas em recursos

O 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 ao cofre de backup controlam o acesso do usuário ao usar APIs do AWS Backup. 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. Você pode criar políticas de acesso separadas no IAM que controlam o acesso a essas APIs, a fim de controlar totalmente o acesso aos backups.

Para saber como criar uma política de acesso para cofres de backup, consulte [Definindo políticas de acesso em cofres de backup e pontos de recuperação \(p. 36\)](#).

Funções de serviço IAM

Uma AWS Identity and Access Management (IAM) função do (IAM) é muito semelhante a um usuário, ao ser uma AWS identidade com políticas de permissão que determinam o que a identidade pode e não pode fazer na AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, uma função destina-se a ser assumida por qualquer pessoa que precisar dela. Uma função de serviço é uma função que um AWS serviço assume a realização de 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 funções do IAM, consulte [Funções do IAM](#) no Manual do usuário do IAM.

A função que você transmite ao AWS Backup deve ter uma política do IAM com as permissões que habilitam o AWS Backup a executar ações associadas às operações de backup, como criação, restauração ou expiração de backups. Diferentes permissões são necessárias para cada um dos AWS serviços que o AWS Backup oferece suporte ao. A função também deve ter o AWS Backup listado como uma entidade confiável, o que permite que o AWS Backup assumir a função.

Quando você atribui recursos a um plano de backup, ou se você executar um backup sob demanda, cópia ou restauração, você deve passar uma função de serviço que tenha acesso para executar as operações subjacentes nos recursos especificados. O AWS Backup usa essa função para criar, marcar e excluir recursos em sua conta.

O uso do AWS Funções para controlar o acesso a 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 apenas conceda permissões para fazer backup de bancos de dados do Amazon Relational Database Service (Amazon RDS) e apenas conceda aos proprietários dos bancos de dados a permissão para transmitir essa função ao AWS Backup. O 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 de serviços que tenham as permissões corretas que o AWS Backup necessita.

Para obter mais informações sobre as políticas gerenciadas do AWS Backup, consulte [Políticas gerenciadas \(p. 104\)](#).

Função de serviço padrão para AWS Backup

Ao usar o AWS Backup Console pela primeira vez, você pode optar por ter o AWS Backup criar uma função de serviço padrão para você. Esta função tem as permissões que o AWS Backup precisa executar operações de backup para todos os AWS serviços que ele suporta. Para escolher a função de serviço padrão, siga qualquer uma das opções em [Conceitos básicos](#).

Note

Você deve criar a função padrão usando o AWS Console de gerenciamento. Não é possível criar a função padrão usando a função AWS Interface de linha de comando (AWS CLI).

Se você preferir usar funções personalizadas, como funções separadas para diferentes tipos de recursos, também poderá fazer isso e transmitir suas funções personalizadas ao AWS Backup. Para exibir exemplos de funções que habilitam o backup e a restauração para tipos de recursos individuais, consulte a tabela no final de [políticas gerenciadas pela](#).

A função de serviço padrão criada pelo AWS Backup gerencia a criação e restauração de backups. Ele tem duas políticas gerenciadas, o `AWSBackupServiceRolePolicyForBackup` e o `AWSBackupServiceRolePolicyForRestores`.

Para restaurar uma instância do Amazon EC2, é necessário inicializar uma nova instância. Para isso, você deve incluir manualmente o `"Action": "iam:PassRole"` no seu papel.

AWS Backup Função de serviço padrão para backups

Essa função inclui uma política do IAM que concede o AWS Backup permissões para descrever o recurso que está sendo submetido a backup, a capacidade de criar, excluir ou descrever um backup e a capacidade de adicionar tags ao backup. Essa política do IAM inclui as permissões necessárias para todos os tipos de recursos que o AWS Backup oferece suporte ao

AWS Backup Função de serviço padrão para restaurações

Essa função inclui uma política do IAM que concede o AWS Backup permissões para criar, excluir ou descrever o novo recurso que está sendo criado a partir de um backup. Ele também inclui permissões para marcar o recurso recém-criado. Essa política do IAM inclui as permissões necessárias para todos os tipos de recursos que o AWS Backup oferece suporte ao

Políticas gerenciadas para o AWS Backup

Políticas gerenciadas

As políticas gerenciadas são políticas independentes baseadas em identidade que você pode anexar a vários usuários, grupos e funções na sua AWS conta.

As políticas gerenciadas do AWS Backup oferecem uma experiência pronta para uso para o AWS Backup

Políticas gerenciadas pelo cliente oferecem controles detalhados para definir o acesso aos backups no AWS Backup. Por exemplo, você pode usá-los para dar ao administrador de backup do banco de dados acesso aos backups do Amazon RDS, mas não aos do Amazon EFS.

Para obter atualizações para as políticas gerenciadas do, consulte [Atualizações da política](#).

As políticas gerenciadas pela AWS

Uma política gerenciada pela AWS é uma política independente que é criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões para vários casos de uso comuns. As políticas gerenciadas pela AWS facilitam a atribuição de permissões apropriadas a usuários, grupos e funções em comparação com a elaboração de suas próprias políticas.

No entanto, não é possível alterar as permissões definidas no AWS Políticas gerenciadas do AWS. A AWS ocasionalmente atualiza as permissões definidas em uma AWS Política gerenciada. Quando isso ocorre, a atualização afetará todas as principais entidades (usuários, grupos e funções) às quais a política está anexada.

AWS Backup fornece várias AWS Políticas gerenciadas para casos de uso comuns do AWS. 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 transmite 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 no console do IAM.

Nome da política	Nome da política gerenciada pelo IAM	Descrição
Política Backup IAM para o administrador	AWSBackupFullAccess (AWSBackupAdminPolicy está obsoleto)	O administrador de backup tem acesso completo ao AWS Backup operações, incluindo criação ou edição de planos de backup, atribuição de recursos para planos de backup e 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 recursos do AWS são atribuídos ao plano apropriado.
Política do para operador de backup do	AWSBackupOperatorAccess (AWSBackupOperatorPolicy está obsoleto)	Os operadores de backup são usuários que devem assegurar que os recursos aos quais eles são responsáveis são submetidos corretamente ao backup. Operadores de backup têm permissões para atribuir recursos para os planos de backup que o administrador de backup cria. Eles também têm permissões para criar backups sob demanda de 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

Nome da política	Nome da política gerenciada pelo I	Descrição
		os tipos de recursos que um operador de backup pode atribuir a um plano de backup ou de restauração a partir de um backup. Isto é feito permitindo que apenas determinadas funções de serviço sejam passadas para um AWS Backup que tenham permissões para um determinado tipo de recurso.
Política do AWS Organizations para o administrador de backup	AWSBackupOrganizationAdminAccess	O administrador da organização tem acesso total às operações do AWS Organizations, incluindo a criação, edição ou exclusão de políticas de backup, a atribuição de políticas de backup a contas e unidades organizacionais e o 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.
Política de função de serviço padrão para backups	AWSBackupServiceRolePolicyForBackup	Concede ao AWS Backup permissões para criar backups de todos os tipos de recursos compatíveis em seu nome.
Política de função de serviço padrão para restaurações	AWSBackupServiceRolePolicyForRestore	Concede ao AWS Backup permissões para restaurar backups de todos os tipos de recursos compatíveis em seu nome. Para restaurações de instância do EC2, você também deve incluir as seguintes permissões para iniciar a instância do EC2: <div> <pre> "Action": "iam:PassRole", "Resource": "arn:aws:iam::account-id:role/role-name", "Effect": "Allow" </pre> </div>

Políticas gerenciadas pelo cliente

Você pode criar políticas independentes que você administra em sua conta AWS. Essas políticas são conhecidas como políticas gerenciadas pelo cliente. Em seguida, você pode anexar as políticas a várias entidades principais na sua conta da AWS. Ao anexar uma política a uma entidade principal, você atribui à entidade as permissões que estão definidas na política.

Uma forma de criar uma política gerenciada pelo cliente é começar copiando uma AWS Política gerenciada. Dessa forma, você sabe que a política está correta no início e basta personalizá-la para seu ambiente.

As seguintes políticas do especificam permissões de backup e restauração para AWS Serviços da . Eles podem ser personalizados e anexados a funções que você criar para limitar ainda mais o acesso ao AWS recursos da AWS.

Políticas de backup e restauração para o indivíduo AWS Serviços

Política
de
restauração
de
serviço

Política
de
restauração
do
DynamoDB

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
  
      "Action": [  
  
        "dynamodb:DescribeBackup",  
  
        "dynamodb:DescribeBackup",
```

Política
de
restauração
de
serviço

```
1,  
  "dynamodb:RestoreTableFromBackup",  
  
  "Resource": "arn:aws:dynamodb:*:*:table/  
*",  
  
  "dynamodb:Scan",  
  
  "Effect": "Allow"  
},  
  "dynamodb:Query",  
  
  {  
  
    "dynamodb:UpdateItem",  
    "Action":  
[  
  
    "dynamodb:PutItem",  
    "tag:GetResources"  
  
    ],  
    "dynamodb:GetItem",  
  
    "Resource": "*",  
    "dynamodb>DeleteItem",
```

Política
de
backup
de
serviço

```
"Effect": "Allow"

"dynamodb:BatchWriteItem"
},

{
  1,

  "Action":
[ "Resource": "arn:aws:dynamodb:*:*:table/
*",

  "Effect": "Allow"
"dynamodb:DescribeBackup",

},

{
  "dynamodb>DeleteBackup"

  "Action":
[],

  "Resource": "arn:aws:dynamodb:*:*:table/
*/
dynamodb:RestoreTableFromBackup",
*",

  "Effect": "Allow"
"dynamodb>DeleteBackup"

},
```

Política
de
backup
de
serviço

```
],
{

  "Resource": "arn:aws:dynamodb:*:*:table/
*/Effect": "Allow",
  backup/
  *,

  "Action":
  [
    "Effect": "Allow"

  ]
} "backup:DescribeBackupVault",

"backup:CopyIntoBackupVault"

],

"Resource": "arn:aws:backup:*:*:backup-
vault:*"

}

]
}
```

Política
de
backup
de
serviço

Política
de
backup
do
Amazon
EBS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "ec2:CreateVolume",
    },
    {
      "ec2>DeleteVolume",
      "Effect": "Allow",
    },
  ],
  "Action": [
```

Política
de
backup
de
serviço

```
"Resource":
[

    "ec2:CreateSnapshot",
    "arn:aws:ec2:*::snapshot/*",

    "ec2:DeleteSnapshot"

    "arn:aws:ec2:*::volume/*"
],

]

"Resource":
[
],

{

    "arn:aws:ec2:*::snapshot/*",

    "Effect": "Allow",

    "Actions": "ec2:*::volume/*"
}

]

"ec2:DescribeSnapshots",

},
```

Política
de
backup
de
serviço

```
{
  "ec2:DescribeVolumes"

  "Effect": "Allow",
},

  "Action":
[
  "Resource": "*"

}
]
} "ec2:DescribeVolumes",

"ec2:DescribeSnapshots",

"ec2:CopySnapshot",

"ec2:DescribeTags"

],

"Resource": "*"
}
```

Política
de
backup
de
serviço

```
},  
  
{  
  
  "Action":  
  [  
  
    "tag:GetResources"  
  
  ],  
  
  "Resource": "*",  
  
  "Effect": "Allow"  
  
},  
  
{  
  
  "Effect": "Allow",
```


Política
de
backup
de
serviço

```
"Action":  
[  
  
  "backup:DescribeBackupVault",  
  
  "backup:CopyIntoBackupVault"  
  
],  
  
  "Resource": "arn:aws:backup:*:*:backup-  
vault:*"  
  
}  
  
]
```

Política
de
backup
de
serviço

Política
de
backup
do
Amazon
EFS

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "elasticfilesystem:Backup",  
        "elasticfilesystem:Restore",  
        "elasticfilesystem:DescribeTags",  
        "elasticfilesystem:CreateFilesystem",  
        "elasticfilesystem:DescribeFilesystems"  
      ],  
      "Resource": "arn:aws:elasticfilesystem:*:*:file-  
system/  
*"  
    }  
  ]  
}
```

Política
de
backup
de
serviço

```
"Effect": "Allow"
"elasticfilesystem:DeleteFilesystem"
},
],
{
  "Resource": "arn:aws:elasticfilesystem:*:*:file-
system/
*"
}
]
} "tag:GetResources"
],
{
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Effect": "Allow",
```

Política
de
backup
de
serviço

```
"Action":  
[  
  
  "backup:DescribeBackupVault",  
  
  "backup:CopyIntoBackupVault"  
  
],  
  
  "Resource": "arn:aws:backup:*:*:backup-  
vault:*"  
  
}  
  
]  
}
```

Política de backup do Amazon RDS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:AddTagToDBInstances",
        "rds:DeleteTagsFromSnapshots",
        "rds:DeleteTagsFromSnapshots",

```

Política
de
backup
de
serviço

```
"rds:RestoreDBSnapshotFromDBSnapshot",
```

```
"rds:CopyDBSnapshot",
```

```
"rds:AddTagsToDBInstances",
```

```
],
```

```
"rds:CreateDBClusterSnapshot",
```

```
"rds:DescribeDBClusters",
```

```
"rds:DescribeDBClusterSnapshots",
```

```
]
```

```
}
```

```
"rds:CopyDBClusterSnapshot"
```

```
],
```

```
"Resource": "*"
```

```
},
```

Política
de
backup
de
serviço

```
{

  "Effect": "Allow",

  "Action": [

    "rds:DeleteDBSnapshot",

    "rds:ModifyDBSnapshotAttribute"

  ],

  "Resource": [

    "arn:aws:rds:*:*:snapshot:awsbackup:*"

  ]
}
```

Política
de
backup
de
serviço

```
    },  
  
    {  
  
      "Effect":  
        "Allow",  
  
      "Action":  
        [  
  
          "rds:DeleteDBClusterSnapshot",  
  
          "rds:ModifyDBClusterSnapshotAttribute"  
        ],  
  
      "Resource":  
        [  
  
          "arn:aws:rds:*:*:cluster-  
snapshot:awsbackup:*"  
        ],  
  
    },  
  
    {  
  
      "Action":  
        [  

```


Política
de
backup
de
serviço

```
"tag:GetResources"
```

```
],
```

```
"Resource": "*",
```

```
"Effect": "Allow"
```

```
},
```

```
{
```

```
"Effect": "Allow",
```

```
"Action":
```

```
[
```

```
"backup:DescribeBackupVault",
```

Política
de
backup
de
serviço

```
"backup:CopyIntoBackupVault"

],

"Resource": "arn:aws:backup:*:*:backup-
vault:*"

},

{

"Action": "kms:DescribeKey",

"Effect": "Allow",

"Resource": "*"

}

]
```

Política
de
backup
de
serviço

Política
de
backup
do
Amazon
Aurora

```
{  
  
  "Version": "2012-10-17",  
  "Statement": [  
  
    {  
  
  
  
      "Effect": "Allow",  
  
  
      "Action": [  
  
  
  
  
  
  
  
  
        "rds:CreateDBClusterSnapshot",  
  
  
  
  
  
  
  
  
  
        "rds:DescribeDBClusters",  
  
  
  
  
  
  
  
  
  
        "rds:RestoreDBClusterFromSnapshot",  
  
      ]  
    }  
  ]  
}
```

Política
de
backup
de
serviço

```
"rds:AddTagsToResource",  
  
"rds:AddTagsToResource",  
  
],  
"rds:CopyDBClusterSnapshot"  
  
"Resource": "*" ],  
}  
]  
}  
"Resource": "*" ],  
  
{  
  
"Effect": "Allow",  
  
"Action": [  
]
```

Política
de
backup
de
serviço

```
"rds:DeleteDBClusterSnapshot"

],

"Resource":
[

"arn:aws:rds:*:*:cluster-
snapshot:awsbackup:*"

]

},

{

"Action":
[

"tag:GetResources"
```

Política
de
backup
de
serviço

```
],  
  
  "Resource": "*",  
  
  "Effect": "Allow"  
},  
  
{  
  
  "Effect": "Allow",  
  
  "Action": [  
  
    "backup:DescribeBackupVault",  
  
    "backup:CopyIntoBackupVault"  
  ],  

```

Política
de
backup
de
serviço

```
"Resource": "arn:aws:backup:*:*:backup-  
vault:*"  
  
},  
  
{  
  
  "Action": "kms:DescribeKey",  
  
  "Effect": "Allow",  
  
  "Resource": "*" }  
]  
}
```

Política
de
backup
de
serviço

Política
de
backup
do
AWS
Storage
Gateway

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
  
      "Effect": "Allow",  
  
      "Action": [  
  
        "storagegateway:DeleteSnapshot",  
  
        "storagegateway:DescribeSnapshots",  
  
        "storagegateway:DescribeStorediSCSIVolumes",  
  
      ],  
      "storagegateway:DescribeStorediSCSIVolumes"
```


Política de backup de serviço

```

    "Resource": "arn:aws:storagegateway:*:*:gateway/
*/
volume/
*",

    },
    "Resource": "arn:aws:storagegateway:*:*:gateway/
*/
volume/
*",

    },
    "Effect": "Allow",
    {

    "Action":
    [
    "Effect": "Allow",

    "Action":
    [ "ec2:CreateTags",

    "ec2:DescribeSnapshots",
    "storagegateway:DescribeGatewayInformation",

    ],
    "storagegateway:CreateStorediSCSIVolume",

    "Resource": "arn:aws:ec2:*:*:snapshot/
*"

    "storagegateway:CreateCachediSCSIVolume"
    },

```

Política
de
backup
de
serviço

```
{
  ],

  "Effect": "Allow",
  "Resource": "arn:aws:storagegateway:*:*:gateway/
*"

  "Action":
  [
    ],

    {

      "ec2:DescribeSnapshots"

      "Effect": "Allow",

    ],

    "Action":
    [

      "Resource": "*"

    ],
    "storagegateway:ListVolumes"

    {

    ],

    "Action":
    [

      "Resource": "arn:aws:storagegateway:*:*:*"

    ]
  ]
}
```

Política
de
backup
de
serviço

```
}
"tag:GetResources"

],

"Resource": "*",

"Effect": "Allow"

},

{

"Effect": "Allow",

"Action":

[

"backup:DescribeBackupVault",

"backup:CopyIntoBackupVault"
```

Política
de
backup
de
serviço

```
[  
  {  
    "Resource": "arn:aws:backup:*:*:backup-  
vault:*"  
  }  
]
```

Política
de
backup
de
serviço

Política
de
backup
do
Amazon
FSx

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "fsx:DescribeBackups",
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Action": "fsx:CreateFilesystemFromBackup",
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Política
de
backup
de
serviço

```
"Effect":  
"Allow",  
  
[  
  
  {  
  
    "arn:aws:fsx:*:*:file-  
system/*",  
    "arn:aws:fsx:*:*:file-  
system/  
*",  
  
    "arn:aws:fsx:*:*:backup/  
*",  
    "arn:aws:fsx:*:*:backup/  
*" ,  
  
  ]  
],  
  
{  
  
  {  
  
    "Action":  
    "fsx:DescribeFileSystems",  
    "Action":  
    "fsx:DescribeFileSystems",  
  
    "Effect":  
    "Allow",
```

Política de backup de serviço

```
"Effect":
"Allow",

"Resource":
"arn:aws:fsx:*:*:file-system/*",
},
},
{

{
"Action":
"fsx:ListTagsForResource",

"Action":
"fsx:DescribeBackups",
"Effect":
"Allow",

"Effect":
"Allow",
"Resource":
"arn:aws:fsx:*:*:file-system/*",

"Resource":
"arn:aws:fsx:*:*:backup/*",

},

{
"Action":
"fsx>DeleteBackup",
```

Política
de
backup
de
serviço

```
"Effect":
"Allow",

[
  "Resource":
  "arn:aws:fsx:*:*:backup/
  *",

  },
  "fsx:DeleteFileSystem",

{

  "fsx:UntagResource"
  "Effect":
  "Allow",

  ],
  "Action":
  [

    "Effect":
    "Allow",

    "fsx:ListTagsForResource",

    "Resource":
    "arn:aws:fsx:*:*:file-
system/
  *",

    "fsx:ManageBackupPrincipalAssociations",

    "Condition":

    "fsx:CopyBackup",
    {
```


Política
de
backup
de
serviço

```
"fsx:TagResource"

"Null":

],

{

  "Resource":
  "arn:aws:fsx:*:*:backup/
*"

}

  "aws:ResourceTag/
aws:backup:source-
resource":
  "false"

}

}

},

{
```

**Política
de
backup
de
serviço**

```
"Action":  
  "ds:DescribeDirectories",  
  
"Effect":  
  "Allow",  
  
"Resource":  
  "*" }  
]  
}
```

Política
de
backup
de
serviço

Política
de
backup
do
Amazon
EC2

```
{  
  
  "Version": "2012-10-17",  
  "Statement": [  
  
    {  
  
  
      "Effect": "Allow",  
  
  
      "Action": [  
  
  
        "ec2:CreateVolume",  
  
  
        "ec2:DeleteSnapshot"  
  
      ],  
    },  
  ],  
}
```

Política
de
backup
de
serviço

```
"Resource": "arn:aws:ec2:*::snapshot/"
{
  },
  {
    "arn:aws:ec2:*::snapshot/"
    "*"
    "Effect": "Allow",
    "arn:aws:ec2:*::volume/"
    "*"
    "Action":
    [
    ]
  },
  "ec2:CreateImage",
  {
    "ec2:DeregisterImage"
    "Effect": "Allow",
  ],
  "Action":
  [
    "Resource": "*"
    "ec2:DescribeSnapshots",
  ]
}
```

Política
de
backup
de
serviço

```
"ec2:DescribeVolumes"
"Effect": "Allow",

],
"Action":
[

"Resource": "*"

},
"ec2:CopyImage",

{

"ec2:CopySnapshot"
"Effect": "Allow",

],
"Action":
[

"Resource": "*"

},
"ec2:DescribeImages",

{

"ec2:DescribeInstances"
"Effect": "Allow",

],
```

Política
de
backup
de
serviço

```
"Action":
[

  "Resource": "*"

},
"ec2:CreateTags"

{

},

"Action":
[

  "Resource": "arn:aws:ec2:*:*:image/*"

},
"ec2:RunInstances"

{

},

"Effect": "Allow",

"Effect": "Allow",

"Action":
[

  "Resource": "*"

},
"ec2:DescribeSnapshots",

{
```

Política
de
backup
de
serviço

```

    "Action": "ec2:DescribeTags",
    [

    "ec2:DescribeImages",
    "ec2:TerminateInstances"

    ],
    "ec2:DescribeInstances",

    "Effect": "Allow",

    "ec2:DescribeInstanceAttribute",

    "Resource": "arn:aws:ec2:*:*:instance/*",

    "ec2:DescribeInstanceCreditSpecifications",

    {

    "ec2:DescribeNetworkInterfaces",

    "Action": "iam:PassRole",

    "Resource": "arn:aws:iam::*:role/*",
    "Effect": "Allow",
    "Principal": "AWS",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalAccount": {
                "arn:aws:iam::*:role/*"
            }
        }
    }
    },

    "ec2:DescribeSpotInstanceRequests"

    "Effect": "Allow"

```

Política
de
backup
de
serviço

```
}  
1,  
}  
  
"Resource": "*"   
  
},  
  
{  
  
"Effect": "Allow",  
  
"Action":  
[  
  
"ec2:CreateSnapshot",  
  
"ec2:DeleteSnapshot",  
  
"ec2:DescribeVolumes",
```


Política
de
backup
de
serviço

```
"ec2:DescribeSnapshots"

],

"Resource":
[

"arn:aws:ec2:*::snapshot/
*",

"arn:aws:ec2:*::volume/
*"

]

},

{

"Action":
[
```

Política
de
backup
de
serviço

```
"tag:GetResources"
```

```
],
```

```
"Resource": "*",
```

```
"Effect": "Allow"
```

```
},
```

```
{
```

```
"Effect": "Allow",
```

```
"Action":
```

```
[
```

```
"backup:DescribeBackupVault",
```

Política
de
backup
de
serviço

```
"backup:CopyIntoBackupVault"  
  
],  
  
"Resource": "arn:aws:backup:*:*:backup-  
vault:*"  
  
}  
]  
}
```

Política
de
backup
de
serviço

Política
de
cópia
de
Backup
do
Windows
VSS
(Volume
Shadow
Copy
Service)

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
  
      "Effect": "Allow",  
  
      "Action": [  
  
        "ec2:CreateTags",  
  
        "ec2:DeleteSnapshot"
```

Política
de
backup
de
serviço

```
],  
  
  "Resource": "arn:aws:ec2:*::snapshot/  
*",  
  
},  
  
{  
  
  "Effect": "Allow",  
  
  "Action": [  
  
    "ec2:CreateImage",  
  
    "ec2:DeregisterImage"  
  
  ],  
  
  "Resource": "*" }
```

Política
de
backup
de
serviço

```
    },  
  
    {  
  
        "Effect": "Allow",  
  
        "Action": [  
  
            "ec2:CopyImage",  
  
            "ec2:CopySnapshot"  
  
        ],  
  
        "Resource": "*"   
  
    },  
  
    {
```

Política
de
backup
de
serviço

```
"Effect": "Allow",

"Action":
[

    "ec2:CreateTags"

],

"Resource": "arn:aws:ec2:*:*:image/*"

},

{

    "Effect": "Allow",

    "Action":
[
```

Política
de
backup
de
serviço

```
"ec2:DescribeSnapshots",  
  
"ec2:DescribeTags",  
  
"ec2:DescribeImages",  
  
"ec2:DescribeInstances",  
  
"ec2:DescribeInstanceAttribute",  
  
"ec2:DescribeInstanceCreditSpecifications",  
  
"ec2:DescribeNetworkInterfaces",  
  
"ec2:DescribeElasticGpus",
```


Política
de
backup
de
serviço

```
"ec2:DescribeSpotInstanceRequests"
```

```
],
```

```
"Resource": "*"
```

```
},
```

```
{
```

```
"Effect": "Allow",
```

```
"Action":
```

```
[
```

```
"ec2:CreateSnapshot",
```

```
"ec2>DeleteSnapshot",
```

Política
de
backup
de
serviço

```
"ec2:DescribeVolumes",

"ec2:DescribeSnapshots"

],

"Resource":
[

"arn:aws:ec2:*::snapshot/
*",

"arn:aws:ec2:*::volume/
*"

],

},

{
```

Política
de
backup
de
serviço

```
"Action":  
[  
  
  "tag:GetResources"  
  
  ],  
  
  "Resource": "*",  
  
  "Effect": "Allow"  
  
},  
  
{  
  
  "Effect": "Allow",  
  
  "Action":  
[
```

Política
de
backup
de
serviço

```
"backup:DescribeBackupVault",

"backup:CopyIntoBackupVault"

],

"Resource": "arn:aws:backup:*:*:backup-
vault:*"

},

{

"Effect": "Allow",

"Action":
[

"ssm:CancelCommand",
```

Política
de
backup
de
serviço

```
"ssm:GetCommandInvocation"

],

"Resource": "*"

},

{

"Effect": "Allow",

"Action": "ssm:SendCommand",

"Resource": [

"arn:aws:ssm:*:*:document/

AWSEC2-

CreateVssSnapshot",
```

Política de restauração de serviço

```
"arn:aws:ec2:*:*:instance/  
*"
]
}
]
```

Para restaurar um backup criptografado, execute um dos seguintes procedimentos:

- Lista de permissões de sua função no AWS Key Management Service (AWS KMS), ou
- Anexe esta política à sua função do IAM para restaurações:

```
{  
  "Action": [  
    "kms:DescribeKey",  
    "kms:Decrypt",  
    "kms:Encrypt",  
    "kms:GenerateDataKey",  
    "kms:ReEncrypt",  
  ],  
  "Effect": "Allow",  
  "Resource": "*"
}
```

Funções vinculadas ao serviço para o AWS Backup

O AWS Backup usa [funções vinculadas a serviços AWS Identity and Access Management \(IAM\)](#). A função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao AWS Backup. Não confunda a função vinculada ao serviço com o som semelhante. Função de serviço do, como a função AWS Backup no console cria ao criar um novo plano de backup.

O AWS Backup A função vinculada ao serviço do é `AWSBackupServiceLinkedRolePolicyForBackup`.

O AWS Backup Usa essa função vinculada ao serviço em apenas duas situações:

- Para backup entre contas, a conta de destino usa uma função vinculada ao serviço para extrair backups no cofre de destino.
- Para backup automático do Amazon EFS.

As funções vinculadas a serviços são predefinidas pelo AWS Backup e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome. Para atualizações AWS BackupO faz com que as permissões de função vinculada ao serviço do, consulte [Atualizações da política](#). Não é possível editar permissões de função vinculada ao serviço.

Uma função vinculada ao serviço facilita a configuração do AWS Backup porque dispensa a inclusão manual das permissões necessárias. O AWS Backup define as permissões de suas funções vinculadas ao serviço e, a menos que definido em contrário, somente o AWS Backup pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Criar uma função vinculada ao serviço para o AWS Backup

Você não precisa criar manualmente uma função vinculada a serviço. Quando você configura o gerenciamento entre contas ou o backup automático do Amazon EFS no AWS Management Console, o AWS CLI, ou o AWS API, AWS BackupO cria a função vinculada ao serviço para você.

Editar uma função vinculada ao serviço para o AWS Backup

AWS BackupO não permite que você edite a função vinculada ao serviço de backup. Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, você poderá editar a descrição da função usando o IAM. Para obter mais informações, consulte [Editar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Backup

Você pode usar o console do IAM, o AWS CLI ou o AWS Para excluir manualmente a função vinculada ao serviço. Para fazer isso, você deve primeiro usar o console ou a API do Amazon EFS para limpar a caixa de seleção Backup automático para desativar o backup automático dos sistemas de arquivos do Amazon EFS.

Note

Se o AWS BackupO serviço está usando a função vinculada ao serviço quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir a função vinculada ao serviço de backup

1. Use o console do Amazon EFS para limpar a caixa de seleção Backup automático para desativar o backup automático dos sistemas de arquivos do Amazon EFS. Ou use o Amazon EFS Put Backup Policy API para desativar backups automáticos.

Quando não houver mais sistemas de arquivos do Amazon EFS selecionados para fazer backup automaticamente, você pode excluir a função vinculada ao serviço.

2. Use o console do IAM, o AWS CLI, ou o AWS Para excluir a função vinculada ao serviço de backup. Para obter mais informações, consulte [Excluir uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Uma vez que a função vinculada ao serviço é excluída, o AWS Backup removerá a seleção de backup desses recursos.

Regiões compatíveis com funções vinculadas ao serviço do AWS Backup

O AWS Backup oferece suporte a funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte [AWS Backup Regiões e endpoints do AWS](#) Referência geral.

Atualizações de políticas do AWS Backup

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. É necessário tempo e experiência para [criar políticas gerenciadas pelo cliente do IAM](#) que fornecem à sua equipe apenas as permissões de que precisam. Para começar a usar rapidamente, você pode usar nosso [AWS Políticas gerenciadas do](#).

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada pela AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

Além disso, a AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política gerenciada pela AWS denominada `ReadOnlyAccess` fornece acesso somente leitura a todos os serviços e recursos da AWS. Quando um serviço executa um novo recurso, a AWS adiciona permissões somente leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte [Políticas gerenciadas pela AWS para funções de trabalho](#) no Manual do usuário do IAM.

Visualize detalhes sobre atualizações do AWS Políticas gerenciadas do para o AWS Backup desde que este serviço começou a acompanhar essas alterações. Para receber alertas automáticos sobre alterações nessa página, inscreva-se no feed RSS no AWS Backup Página Histórico de documentos.

Alteração	Descrição	Data
AWSBackupFullAccess — Adicionada permissão para criar uma função vinculada ao serviço	AWS BackupAdicionado <code>iam:CreateServiceLinkedRole</code> para criar uma função vinculada ao serviço (na base do melhor esforço) para automatizar a exclusão de pontos de recuperação expirados para você. Sem essa função vinculada ao serviço, o AWS Backup não pode excluir pontos de recuperação expirados depois que os clientes excluem	5 de julho de 2021

Alteração	Descrição	Data
	<p>a função original do IAM que usaram para criar seus pontos de recuperação.</p> <p>AWS Backup precisava desta permissão como parte do <code>DeleteRecoveryPoint</code> Operação da API.</p>	
<p>AWSBackupServiceLinkedRolePolicy — Adicionada permissão para dar suporte à exclusão de pontos de recuperação do DynamoDB</p>	<p>AWS Backup adicionou a nova ação <code>dynamodb:DeleteBackup</code> para automatizar a exclusão de pontos de recuperação do DynamoDB expirados com base nas configurações do ciclo de vida do plano de backup.</p> <p>AWS Backup precisava dessa permissão para excluir tabelas do DynamoDB como parte do <code>DeleteRecoveryPoint</code> Operação da API.</p>	5 de julho de 2021
<p>AWSBackupOperatorAccess — Ações redundantes removidas</p>	<p>AWS Backup removeu as ações existentes <code>backup:GetRecoveryPointRestoreMetadata</code> e <code>erds:DescribeDBSnapshots</code> eram redundantes.</p> <p>AWS Backup Não foi necessário que ambos <code>osbackup:GetRecoveryPointRestoreMetadata</code> e <code>backup:Get*</code> Como parte do <code>AWSBackupOperatorAccess</code> AWS Política gerenciada. Além disso, AWS Backup Não foi necessário que ambos <code>osrds:DescribeDBSnapshots</code> e <code>erds:describeDBSnapshots</code> Como parte do <code>AWSBackupOperatorAccess</code> AWS Política gerenciada.</p>	25 de maio de 2021
<p>AWSBackupOperatorPolicy — Ações redundantes removidas</p>	<p>AWS Backup removeu as ações existentes <code>backup:GetRecoveryPointRestoreMetadata</code> e <code>erds:DescribeDBSnapshots</code> eram redundantes.</p> <p>AWS Backup Não foi necessário que ambos <code>osbackup:GetRecoveryPointRestoreMetadata</code> e <code>backup:Get*</code> Como parte do <code>AWSBackupOperatorPolicy</code> AWS Política gerenciada. Além disso, AWS Backup Não foi necessário que ambos <code>osrds:DescribeDBSnapshots</code> e <code>erds:describeDBSnapshots</code> Como parte do <code>AWSBackupOperatorPolicy</code> AWS Política gerenciada.</p>	25 de maio de 2021

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup Adicionada permissão para aplicar tags a restaurações do Amazon FSx	AWSBackupServiceRolePolicyForBackup AWS Backup adicionou a nova ação <code>fsx:TagResource</code> para permitir que você aplique tags aos sistemas de arquivos do Amazon FSx durante o processo de restauração. AWS Backup precisava desta permissão para aplicar tags aos sistemas de arquivos do Amazon FSx como parte do <code>StartRestoreJob</code> Operação da API.	24 de maio de 2021
AWSBackupServiceRolePolicyForBackup Adicionada permissão para executar restaurações do Amazon EC2	AWSBackupServiceRolePolicyForBackup AWS Backup adicionou as novas ações <code>ec2:DescribeImages</code> e <code>ec2:DescribeInstances</code> para permitir que você restaure instâncias do Amazon EC2 a partir de pontos de recuperação. AWS Backup precisava dessa permissão para restaurar instâncias do Amazon EC2 a partir de pontos de recuperação como parte do <code>StartRestoreJob</code> Operação da API.	24 de maio de 2021
AWSBackupServiceRolePolicyForBackup Adicionada permissão para executar cópias entre regiões e entre contas do Amazon FSx	AWSBackupServiceRolePolicyForBackup AWS Backup adicionou a nova ação <code>fsx:CopyBackup</code> para permitir que você copie pontos de recuperação do Amazon FSx entre regiões e contas. AWS Backup precisava dessa permissão para copiar pontos de recuperação do Amazon FSx entre regiões e contas como parte do <code>StartCopyJob</code> Operação da API.	12 de abril de 2021
AWSBackupServiceLinkedRolePolicy Adicionada permissão para perfrom Amazon FSX entre regiões e cópias de contas cruzadas	AWSBackupServiceLinkedRolePolicy AWS Backup adicionou a nova ação <code>fsx:CopyBackup</code> para permitir que você copie pontos de recuperação do Amazon FSx entre regiões e contas. AWS Backup precisava dessa permissão para copiar pontos de recuperação do Amazon FSx entre regiões e contas como parte do <code>StartCopyJob</code> Operação da API.	12 de abril de 2021

Alteração	Descrição	Data
AWSBackupServiceRolePolicyForBackup Adicionadas permissões para dar suporte ao backup criptografado de tabela do DynamoDB	AWS Backup atualizou a sua AWS diretivas gerenciadas para atender ao seguinte requisito: para o AWS Backup para criar um backup de uma tabela criptografada do DynamoDB, você deve adicionar as permissões <code>kms:Decrypt</code> e <code>kms:GenerateDataKey</code> para a função do IAM usada para o backup.	10 de março de 2021
AWSBackupFullAccess Permissões adicionadas ao suporte de backups contínuos do Amazon RDS e restauração Point-In-Time	AWS Backup atualizou a sua AWS Política gerenciada para cumprir os seguintes requisitos: Para usar AWS Backup para configurar backups contínuos para seu banco de dados do Amazon RDS, verifique a permissão da API <code>rds:ModifyDBInstance</code> na função do IAM definida pela configuração do plano de backup. Para restaurar backups contínuos do Amazon RDS, você deve adicionar a permissão <code>rds:RestoreDBInstanceToPointInTime</code> para a função do IAM que você enviou para o trabalho de restauração. No AWS Backup, para descrever o intervalo de tempos disponíveis para recuperação point-in-time, você deve incluir <code>rds:DescribeDBInstanceAutomatedBackups</code> Permissão de API em sua política gerenciada do IAM.	10 de março de 2021
AWS Backup Acompanhar alterações	AWS Backup começou a monitorar as alterações para o seu AWS Políticas gerenciadas do.	10 de março de 2021

Validação de conformidade do AWS Backup

Audidores externos avaliam a segurança e a conformidade do AWS Backup como parte de vários programas de conformidade da AWS, como SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista dos produtos da AWS no escopo de programas de conformidade específicos, consulte [Produtos da AWS no escopo por programa de conformidade](#). Para obter informações gerais, consulte [Programas de conformidade da AWS](#).

Você pode fazer download de relatórios de auditoria externa usando o AWS Artifact. Para obter mais informações, consulte [Download de relatórios no AWS Artifact](#) no AWS Artifact Guia do usuário do.

Sua responsabilidade de conformidade ao usar o AWS Backup é determinada pela confidencialidade de seus dados, pelas metas de conformidade da sua empresa e pelas regulamentações e leis aplicáveis. Caso seu uso do AWS Backup esteja sujeito à conformidade com padrões como HIPAA, PCI ou FedRAMP, a AWS fornecerá os recursos para ajudar:

- [Guias de início rápido de segurança e conformidade](#)— esses guias de implantação abordam as considerações de arquitetura e fornecem etapas para a implantação de ambientes de linha de base concentrados em conformidade e segurança na AWS.
- [Whitepaper Arquitetura para segurança e conformidade com a HIPAA](#): esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações em conformidade com a HIPAA.
- [Recursos de conformidade da AWS](#): esta coleção de manuais e guias pode ser aplicável a seu setor e local.
- [AWS Config](#): este produto da AWS avalia até que ponto suas configurações de recursos atendem adequadamente às práticas internas e às diretrizes e regulamentações do setor.
- [AWS Security Hub](#): esse serviço da AWS fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a verificar sua conformidade com padrões e práticas recomendadas de segurança do setor.

Resiliência no AWS Backup

AWS Backup leva a sua resiliência — e a sua segurança de dados — extremamente a sério.

AWS Backup armazena suas cópias de segurança com a máxima resiliência e durabilidade quanto o original do seu recurso AWS. Você pode armazená-lo lá em cima.

AWS Backup foi projetado para usar a AWS para replicar seus backups em várias zonas de disponibilidade para uma durabilidade de 99,999999999% (11 noves) em um determinado ano, desde que você adira aos [AWS Backup documentação](#).

AWS Backup criptografa seus planos de backup em repouso e faz backup contínuo deles. Também é possível restringir o acesso a seus planos de backup usando o [AWS Identity and Access Management \(IAM\)](#) credenciais e políticas. Para obter mais informações, consulte [Autenticação](#), [Controle de acesso](#), e [Melhores práticas de segurança no IAM](#).

A AWS infraestrutura global é criada ao redor das [AWS Regiões e Zonas de disponibilidade](#). As regiões da AWS fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, altas taxas de transferência e redes altamente redundantes. AWS Backup armazena backups entre Zonas de disponibilidade. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais. Para obter mais informações, consulte [AWS Backup Acordo de Nível de Serviço \(SLA\)](#).

Além disso, AWS Backup permite que você copie seus backups entre regiões para uma resiliência ainda maior. Para obter mais informações sobre o [AWS Backup Recurso de cópia entre regiões](#), consulte [Criar uma cópia de backup](#).

Para mais informações sobre regiões e zonas de disponibilidade da AWS, consulte [Infraestrutura global da AWS](#).

Segurança da infraestrutura no AWS Backup

Como um serviço gerenciado, o AWS Backup é protegido pelos procedimentos de segurança de rede global que são descritos no [Amazon Web Services: Visão geral dos processos de segurança do Whitepaper](#).

Você usa chamadas de API publicadas pela AWS para acessar o AWS Backup por meio da rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos 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 oferece suporte a esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

AWS BackupCotas do

Veja a seguir as cotas de recursos ao trabalhar com o AWS Backup.

Recurso	Quota
Número de cofres de backup por região, por conta da	100
Número de cópias de backup simultâneas (por serviço) para uma região de destino por conta	5*
Número de planos de backup por região, por conta da	100
Número de versões por plano de backup	2.000
Número de jobs de backup ativos por conta	Ilimitado
Número de trabalhos de backup simultâneos por recurso	1
Número de tags de metadados por recurso salvo	50
Número de pontos de recuperação por cofre de backup	1.000.000

*AWS BackupO oferece suporte a até 100 cópias de backup simultâneas das AMIs do Amazon EC2 do para um destinoAWSRegião por conta.

AWS BackupO permite atribuir um número ilimitado de recursos a um plano de backup usando tags. Você pode atribuir até 100 recursos exclusivos a um plano de backup usando nomes de recurso da Amazon (ARNs).

Ao gerenciar backups em várias contas usando Organizations, você pode encontrar cotas que elas impõem. Para essas cotas do, consulte o [Cotações para Organizations](#) no Guia do usuário das Organizations.

Note

Para serviços diferentes do Amazon EFS, você também pode encontrar cotas impostas por esses serviços, incluindo:

- [Amazon Elastic File System](#)
- [Amazon Elastic Block Store](#)
- [Amazon RDS](#)
- [Amazon Aurora](#)
- [Amazon EC2](#)
- [AWS Storage Gateway](#)
- [Amazon DynamoDB](#)
- [Amazon FSx for Lustre](#)
- [Servidor de arquivos Amazon FSx for Windows](#)

Monitoring

AWS Backup funciona com outros AWS para permitir que você monitore suas cargas de trabalho. Essas ferramentas incluem o seguinte:

- Usar o Amazon CloudWatch e Amazon EventBridge para monitorar processos AWS Backup.
 - Você pode usar o CloudWatch para rastrear métricas, criar alarmes e exibir painéis.
 - Você pode usar o EventBridge para exibir e monitorar AWS Backup.

Para obter mais informações, consulte [MonitoramentoAWS BackupEventos usando o EventBridge](#) (p. 169) e [MonitoramentoAWS Backup métricas com o CloudWatch](#) (p. 191).

- Usar o AWS CloudTrail para monitorar chamadas de API AWS Backup. Você pode identificar a hora, o IP de origem, os usuários e as contas que fazem essas chamadas. Para obter mais informações, consulte [Registro em logAWS BackupChamadas de API com CloudTrail](#) (p. 193).
- Usar o Amazon Simple Notification Service (Amazon SNS) para assinar AWS Backup, como eventos de backup, restauração e cópia. Para obter mais informações, consulte [Usando o Amazon SNS para rastrearAWS BackupEventos](#) do (p. 199).

MonitoramentoAWS BackupEventos usando o EventBridge

Tópicos

- [Monitorar eventos usando o EventBridge](#) (p. 169)
- [Diferenças com oAWS BackupAPI de notificação](#) (p. 190)

Monitorar eventos usando o EventBridge

Você pode usar o EventBridge para monitorar AWS Backup. Um caso de uso comum é receber um alarme quando um trabalho de backup falha. AWS Backup emite eventos para o EventBridge de uma forma de melhor esforço a cada 5 minutos.

O objetivo desta página de documentação é fornecer a você os materiais de referência para usar o EventBridge para monitorar AWS Backup. Para saber como controlar eventos usando o EventBridge, consulte [ConfigureAWS Backup eventos para enviar a EventBridge](#) na metade do caminho do blog [Amazon CloudWatch Events e métricas para oAWS Backup](#) ou [Criar uma regra para umAWS Serviço](#) na Guia do usuário do Amazon EventBridge.

Note

Relatar alguns eventos `status: COMPLETED` enquanto outros eventos relatam `state: COMPLETED`. Isso é consistente com o AWS Backup API.

Você pode rastrear o seguinte AWS Backup-eventos relacionados em EventBridge.

Tipo de evento	States	Detalhes do evento
AlterBackup do estado do Job de	ABORTED, COMPLETED, FAILED, EXPIRED, RUNNING, PENDING	accountId, recursos: RecoveryPointArn, details, BackupJobID, BackupSizeInBytes,

Tipo de evento	States	Detalhes do evento
		BackupVaultName, BackupVaultArn, BytsTransferred, CompletionDate, ExpectedCompletionDate, IamroLearn, PercentdOnE, resourceType, StartBy, state, StatusMessage CreatedBy: BackupPlanarn, CreatedBy: BackupPlanID, CreatedBy: BackupPlanVersion, CreatedBy: BackupRuleID
AlterBackup do estado do Job de	CREATED	accountId, recursos: RecoveryPointArn, detalhes, BackupJobID, state, CreationDate
Alterar o estado do Job de cópia	COMPLETED, FAILED, RUNNING	accountId, recursos: RecoveryPointArn, detalhes, BackupSizeInBytes, CompletionDate, CopyJobID, CreationDate, DestinationBackupVaultArn, DestinationRecoveryPointArn, IAMRoLearn, resourceArn, resourceType, state, StatusMessage CreatedBy: BackupPlanarn, CreatedBy: BackupPlanID, CreatedBy: BackupPlanVersion, CreatedBy: BackupRuleID
Alterar o estado do Job de cópia	CREATED	accountId, recursos: RecoveryPointArn, details, state, CreationDate, sourceBackupVaultARN, destinationBackupVaultARN
Restaurar alteração de estado do Job	CREATED, COMPLETED, FAILED, PENDING, RUNNING	accountId, recursos: RecoveryPointArn, details, state, CreationDate, RestoreJobID

Tipo de evento	States	Detalhes do evento
Alteração do estado de recuperação	COMPLETED, PARTIAL, EXPIRED	accountId, recursos: RecoveryPointArn, recursos: BackupVaultArn, details, BackupSizeInBytes, BackupVaultName, CalculatedLifecycle: MoveToColdStorageEat, CompletionDate, CreationDate, EncryptionKeyArn, IAMRoleArn, IsEncrypted, LastoreTime, LastoreTime, LastoreTime, ciclo de vida: ciclo de vida: Dias, ciclo de vida: MoveToColdStorageAfterDays, resourceArn, resourceType, status, StorageClass CreatedBy: BackupPlanArn, CreatedBy: BackupPlanID, CreatedBy: BackupPlanVersion, CreatedBy: BackupRuleID
Restaurar alteração de estado do Job	CREATED	accountId, recursos: RecoveryPointArn, details, state, CreationDate, RestoreJobID
Alteração do estado de recuperação	FAILED, COMPLETED, RUNNING, ABORTED, PENDING	accountId, recursos: RecoveryPointArn, detalhes, BackupSizeInBytes, CompletionDate, CreatedResourceArn, CreationDate, ExpectedCompletionTimeMinutes, IAMRoleArn, PercentDone, RestoreJobID, status, StatusMessage
Alteração do estado de recuperação	MODIFIED, DELETED	accountId, recursos: RecoveryPointArn, recursos: BackupVaultArn, detalhes, ciclo de vida, CalculatedLifecycle, estado
Alteração do estado do backup	CREATED, DELETED, MODIFIED	accountId, recursos: BackupVaultARN, detalhes, BackupVaultName, estado
Alteração do estado das configurações da	MODIFIED	accountId, detalhes, ModifiedAT, estado, ResourceTypeOptInPreference
Alteração do estado de recuperação	MODIFIED, DELETED	accountId, recursos: RecoveryPointArn, recursos: BackupVaultArn, detalhes, ciclo de vida, CalculatedLifecycle, estado

Tipo de evento	States	Detalhes do evento
Alteração do estado do backup	CREATED, DELETED, MODIFIED	accountId, recursos: BackupPlanarn, details, BackupPlanID, versionId, CreationDate, DeletionDate

Use essas cargas JSON de exemplo se quiser usar esses eventos de forma programática.

Estado do evento	Carga útil JSON
Job de backup: FAILED	<pre>{ "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-east-1", "resources": [], "detail": { "backupJobId": "34176239- e96d-4e1d-9fad-529dbb3c3556", "backupVaultArn": "arn:aws:backup:us- west-2:1112233445566:backup- vault:9ab3e749-82c6-4342-9320-5edbf4918b86_beta", "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86_beta", "bytesTransferred": "0", "creationDate": "2020-07-29T20:13:07.392Z", "iamRoleArn": "arn:aws:iam:1112233445566:role/ MockRCBackupIntegTestRole", "resourceArn": "arn:aws:cryo-mock:us- west-2:1112233445566:resource:dummy-fs-1", "resourceType": "CryoTestClient", "state": "FAILED", "statusMessage": "\"Backup job failed because backup vault arn:aws:backup:us- west-2:1112233445566:backup- vault:9ab3e749-82c6-4342-9320-5edbf4918b86_beta does not exist.\"", "startBy": "2020-07-30T04:13:07.392Z", "percentDone": 0 } }</pre>
Job de backup: COMPLETED	<pre>{ "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-east-1", "resources": [</pre>

Estado do evento	Carga útil JSON
	<pre>"arn:aws:backup:us-west-2:1112233445566:recovery-point:f1d966fe-a3bd-410b-b292-99f442d13b56_beta"], "detail": { "backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd", "backupSizeInBytes": "36048", "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9732c1b4-1091-472a-9d9f-52e0565ee39a_beta", "backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a_beta", "bytesTransferred": "36048", "creationDate": "2020-07-15T21:40:31.207Z", "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupIntegTestRole", "resourceArn": "arn:aws:cryo-mock:us-west-2:1112233445566:resource:dummy-fs-1", "resourceType": "CryoTestClient", "state": "COMPLETED", "completionDate": "2020-07-15T21:41:05.921Z", "startBy": "2020-07-16T05:40:31.207Z", "percentDone": 100 } }</pre>

Estado do evento	Carga útil JSON
Job de backup: RUNNING (Em execução)	<pre>{ "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-east-1", "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_beta", "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15_beta", "bytesTransferred": "0", "creationDate": "2020-07-15T21:38:31.152Z", "iamRoleArn": "arn:aws:iam:1112233445566:role/FullBackupIntegTestRole", "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_beta", "backupPlanVersion": "YTkzNmMOMmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5", "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5" } } }</pre>

Estado do evento	Carga útil JSON
Job de backup: ABORTED	<pre>{ "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-east-1", "resources": [], "detail": { "backupJobId": "58cdef95-7680-4c74-80d5-1b64093999c8", "backupVaultArn": "arn:aws:backup:us- west-2:1112233445566:backup- vault:f59bffcd-2538-4bbe-8343-1c60dae27c27_beta", "backupVaultName": "f59bffcd-2538-4bbe-8343-1c60dae27c27_beta", "bytesTransferred": "0", "creationDate": "2020-07-15T21:33:00.803Z", "iamRoleArn": "arn:aws:iam::1112233445566:role/ MockRCBackupIntegTestRole", "resourceArn": "arn:aws:cryo-mock:us- west-2:1112233445566:resource:dummy-fs-1", "resourceType": "CryoTestClient", "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 } }</pre>

Estado do evento	Carga útil JSON
Job de backup: EXPIROU	<pre>{ "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-east-1", "resources": [], "detail": { "backupJobId": "01EE26DC-7107-4D8E-0C54-EAC27C662BA4", "backupVaultArn": "arn:aws:backup:us- west-2:1112233445566:backup-vault:aws/ backup/AutomatedBackupVaultDel2_beta", "backupVaultName": "aws/backup/ AutomatedBackupVaultDel2_beta", "bytesTransferred": "0", "creationDate": "2020-07-29T05:10:20.077Z", "iamRoleArn": "arn:aws:iam::1112233445566:role/ MockRCBackupIntegTestRole", "resourceArn": "arn:aws:cryo-mock:us- west-2:1112233445566:resource.bbd99e4c- e974-489b-94f2-db9e8cc15dd5", "resourceType": "CryoTestClient", "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_beta", "backupPlanVersion": "NjBjOTUzZjYtYzZiNi00Njh1LWlzMTZtNWRjOWY0YTNjN2Vj", "backupPlanRuleId": "3eb0017c- f262-4211-a802-302cebb11dc2" } } }</pre>

Estado do evento	Carga útil JSON
Job de backup: PENDING (PENDENTES)	<pre>{ "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-east-1", "resources": [], "detail": { "backupJobId": "2cffdb68- d6ed-485f-9f9b-8b530749f1c2", "backupVaultArn": "arn:aws:backup:us- west-2:1112233445566:backup- vault:ed1f2661-5587-48bf-8a98- fadb977bf975_beta", "backupVaultName": "ed1f2661-5587-48bf-8a98- fadb977bf975_beta", "bytesTransferred": "0", "creationDate": "2020-07-29T20:01:06.224Z", "iamRoleArn": "arn:aws:iam:1112233445566:role/ MockRCBackupIntegTestRole", "resourceArn": "arn:aws:cryo-mock:us- west-2:1112233445566:resource:testListProtectedResources", "resourceType": "CryoTestClient", "state": "PENDING", "statusMessage": "", "startBy": "2020-07-30T04:01:06.224Z", "percentDone": 0 } }</pre>
Job de backup: CREATED	<pre>{ "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-east-1", "resources": [], "detail": { "backupJobId": "7e8845b5-ca30-415f- a842-e0152bf4d0ca", "state": "CREATED", "creationDate": "2020-06-22T20:32:47.466Z" } }</pre>

Estado do evento	Carga útil JSON
Copiar Job: FAILED	<pre>{ "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-east-1", "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_beta", "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_beta", "destinationRecoveryPointArn": {} } }</pre>

Estado do evento	Carga útil JSON
Copiar Job: RUNNING (Em execução)	<pre>{ "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-east-1", "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- ab60-4fbbabecd3ec_beta", "state": "RUNNING", "destinationBackupVaultArn": "arn:aws:backup:us- west-2::1112233445566:backup- vault:846869de-4589-45c3- ab60-4fbbabecd3ec_beta", "destinationRecoveryPointArn": {}, "createdBy": { "backupPlanId": "b58e3621-1c53-4997- ad8a-afc3347a850e", "backupPlanArn": "arn:aws:backup:us- west-2::1112233445566:backup- plan:b58e3621-1c53-4997-ad8a- afc3347a850e_beta", "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4", "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18" } } }</pre>

Estado do evento	Carga útil JSON
Copiar Job: COMPLETED	<pre>{ "version": "0", "id": "47deb974-6473- aef1-56c2-52c3eaeafceb", "detail-type": "Copy Job State Change", "source": "aws.backup", "account": "1112233445566", "time": "2020-07-15T22:08:04Z", "region": "us-east-1", "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- ab60-4fbbabcbdd3ec_beta", "state": "COMPLETED", "completionDate": "2020-07-15T22:07:58.111Z", "destinationBackupVaultArn": "arn:aws:backup:us- west-2::1112233445566:backup- vault:846869de-4589-45c3- ab60-4fbbabcbdd3ec_beta", "destinationRecoveryPointArn": { "value": "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_beta", "backupPlanVersion": "Mjc4ZTRhMzUtMGESNi00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4", "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18" } } }</pre>

Estado do evento	Carga útil JSON
Copiar Job: CREATED	<pre>{ "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-east-1", "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_beta", "destinationBackupVaultArn": "arn:aws:backup:us- west-2:1112233445566:backup- vault:ef09da5a-21a6-461f- a98f-857e9e621a17_beta" } }</pre>

Estado do evento	Carga útil JSON
Job hos de restauração: FAILED	<pre>{ "version": "0", "id": "296805cc-6ad4-32f2- fb86-4e66c84abce7", "detail-type": "Restore Job State Change", "source": "aws.backup", "account": "1112233445566", "time": "2020-07-15T20:19:29Z", "region": "us-east-1", "resources": ["arn:aws:ec2:us-west-2::image/ ami-06b9894dfb1f9cf48"], "detail": { "restoreJobId": "9B333A28-526B-01CD-4A77-9785A08922FD", "backupSizeInBytes": "22548578304", "creationDate": "2020-07-15T20:19:07.303Z", "iamRoleArn": "arn:aws:iam::1112233445566:role/ CanaryAWSBackupRole", "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." } }</pre>

Estado do evento	Carga útil JSON
Job hos de restauração: RUNNING (Em execução)	<pre>{ "version": "0", "id": "6137a1f0-33f3-99ee- a01a-3d8b96fe2ad6", "detail-type": "Restore Job State Change", "source": "aws.backup", "account": "1112233445566", "time": "2020-07-29T20:26:06Z", "region": "us-east-1", "resources": ["arn:aws:ec2:us-west-2::snapshot/ snap-0fe679ca138cfad2c"], "detail": { "restoreJobId": "F143178C- A866-4782-3B19-BF776A1A790C", "backupSizeInBytes": "3221225472", "creationDate": "2020-07-29T20:26:00.098Z", "iamRoleArn": "arn:aws:iam::1112233445566:role/ OrganizationCanaryTestRole", "percentDone": 0, "resourceType": "EBS", "status": "RUNNING" } }</pre>

Estado do evento	Carga útil JSON
Job hos de restauração: COMPLETED	<pre>{ "version": "0", "id": "8939bc73-dcf1-418c-9420- b9c5e097f0fb", "detail-type": "Restore Job State Change", "source": "aws.backup", "account": "1112233445566", "time": "2020-07-15T03:14:58Z", "region": "us-east-1", "resources": ["arn:aws:rds:us- west-2:1112233445566:snapshot:awsbackup:job- f2494617-4fe0-47e3-969e-a652d902b475"], "detail": { "restoreJobId": "EF332640-02A5-5978-693F-987970F09961", "backupSizeInBytes": "0", "creationDate": "2020-07-15T03:10:01.742Z", "iamRoleArn": "arn:aws:iam::1112233445566:role/ CanaryAWSBackupRole", "percentDone": 0, "resourceType": "RDS", "status": "COMPLETED", "createdResourceArn": "arn:aws:rds:us- west-2:1112233445566:db:cryo- instance7c3d1e78-987e-4450-92e1-3b6dbedb5384", "completionDate": "2020-07-15T03:14:53.128Z" } }</pre>

Estado do evento	Carga útil JSON
Job hos de restauração: PENDING (PENDENTES)	<pre>{ "version": "0", "id": "0586085f-3079- cd79-10b7-908d3c3a21ea", "detail-type": "Restore Job State Change", "source": "aws.backup", "account": "1112233445566", "time": "2020-07-29T20:08:26Z", "region": "us-east-1", "resources": ["arn:aws:backup:us- west-2:1112233445566:recovery- point:42bb8260-92cd-46a2-ab8d- b29f4edb47b1_beta"], "detail": { "restoreJobId": "EB9CE5CB-2B92-8B66- FD16-9829F4DAAAD7", "backupSizeInBytes": "36048", "creationDate": "2020-07-29T20:08:21.083Z", "iamRoleArn": "arn:aws:iam:1112233445566:role/ MockRCBackupIntegTestRole", "percentDone": 0, "resourceType": "CryoTestClient", "status": "PENDING" } }</pre>
Job hos de restauração: CREATED	<pre>{ "version": "0", "id": "af32977e-378f-2122-f985- fca4596f0709", "detail-type": "Restore Job State Change", "source": "aws.backup", "account": "1112233445566", "time": "2020-06-22T18:50:49Z", "region": "us-east-1", "resources": ["arn:aws:backup:us- west-2:1112233445566:recovery- point:f6560d33-3660-494e-8d47- aaba939df32e_beta"], "detail": { "restoreJobId": "267EA62F-C125- EFE5-7099-9D98FC0E422A", "creationDate": "2020-06-22T18:50:46.407Z", "state": "CREATED" } }</pre>

Estado do evento	Carga útil JSON
Ponto de recuperação: COMPLETED	<pre>{ "version": "0", "id": "ec6f75cc-989c-faaf-a642-dd0f1c95bfff0", "detail-type": "Recovery Point Change", "source": "aws.backup", "account": "1112233445566", "time": "2020-07-15T21:39:07Z", "region": "us-east-1", "resources": ["arn:aws:rds:us-west-2:1112233445566:cluster-snapshot:awsbackup:job-4ece7121-d60e-00c2-5c3b-49960142d03b"], "detail": { "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15_beta", "backupVaultArn": "arn:aws:backup:us-west-2:496821122410:backup-vault:e6625738-0655-4aa9-bd37-6ec1dd183b15_beta", "creationDate": "2020-07-15T21:38:31.152Z", "iamRoleArn": "arn:aws:iam:1112233445566:role/FullBackupIntegTestRole", "resourceType": "Aurora", "resourceArn": "arn:aws:rds:us-west-2:1112233445566:cluster:cryo-aurora-14029f40-b0b6-4a61-9fd2-9886f2771add", "status": "COMPLETED", "isEncrypted": "false", "storageClass": "WARM", "completionDate": "2020-07-15T21:39:05.689Z", "createdBy": { "backupPlanId": "bde0f455-4e24-4668-aaaa-4932a97f5cc5", "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:bde0f455-4e24-4668-aaaa-4932a97f5cc5_beta", "backupPlanVersion": "YTkzNmMOMmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5", "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5" }, "lifecycle": { "deleteAfterDays": 100 }, "calculatedLifeCycle": { "deleteAt": "2020-10-23T21:38:31.152Z" } } }</pre>

Estado do evento	Carga útil JSON
Ponto de recuperação: DELETED	<pre>{ "version": "0", "id": "6089ee76-d856-0d7c- cee7-0a431cd43343", "detail-type": "Recovery Point Change", "source": "aws.backup", "account": "1112233445566", "time": "2020-07-29T22:38:49Z", "region": "us-east-1", "resources": ["arn:aws:backup:us- west-2:1112233445566:backup-vault:157f892e- fe46-48da-9dbe-4154f91f8acc_beta", "arn:aws:rds:us- west-2:1112233445566:snapshot:awsbackup:job- cla6d40a-32d1-4d54-bd70-bced933ef107"], "detail": { "state": "DELETED", "lifecycle": { "deleteAfterDays": 300 }, "calculatedLifeCycle": { "deletedAt": "2021-05-25T22:29:02.452Z" } } }</pre>
Ponto de recuperação: MODIFIED	<pre>{ "version": "0", "id": "14365bb1-adeb- bc00-1ee3-8fac188d7996", "detail-type": "Recovery Point Change", "source": "aws.backup", "account": "1112233445566", "time": "2020-07-02T23:33:57Z", "region": "us-east-1", "resources": ["arn:aws:backup:us- west-2:1112233445566:backup- vault:helo12312_beta", "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" } }</pre>

Estado do evento	Carga útil JSON
Cofre de backup: CREATED	<pre>{ "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-east-1", "resources": ["arn:aws:backup:us- west-2:1112233445566:backup- vault:d8864642-155c-4283-a168- a04f40e12c97_beta"], "detail": { "backupVaultName": "d8864642-155c-4283- a168-a04f40e12c97", "state": "CREATED" } }</pre>
Cofre de backup: DELETED	<pre>{ "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-east-1", "resources": ["arn:aws:backup:us- west-2:1112233445566:backup- vault:e8189629-1f8e-4ed2-af7d- b32415d04db1_beta"], "detail": { "backupVaultName": "e8189629-1f8e-4ed2- af7d-b32415d04db1", "state": "DELETED" } }</pre>

Estado do evento	Carga útil JSON
Plano de backup: MODIFIED	<pre>{ "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-east-1", "resources": ["arn:aws:backup:us- west-2:1112233445566:backup- plan:83fcb8ee-2d93-42ac- b06f-591563f3f8de_beta"], "detail": { "backupPlanId": "83fcb8ee-2d93-42ac- b06f-591563f3f8de", "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkkxNDk0", "modifiedAt": "2020-06-24T23:18:19.168Z", "state": "MODIFIED" } }</pre>
Plano de backup: DELETED	<pre>{ "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-east-1", "resources": ["arn:aws:backup:us- west-2:1112233445566:backup- plan:83fcb8ee-2d93-42ac- b06f-591563f3f8de_beta"], "detail": { "backupPlanId": "83fcb8ee-2d93-42ac- b06f-591563f3f8de", "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkkxNDk0", "deletionDate": "2020-06-24T23:18:19.411Z", "state": "DELETED" } }</pre>

Estado do evento	Carga útil JSON
Plano de backup: CREATED	<pre>{ "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-east-1", "resources": ["arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-d3afa4c84f59_beta"], "detail": { "backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59", "versionId": "N2Q4OTczMzEtZmY1My00N2UwLWE3ODUtMjViYWYyOTUzZWY4", "creationDate": "2020-06-24T23:18:15.318Z", "state": "CREATED" } }</pre>
Configuração da região: MODIFIED	<pre>{ "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-east-1", "resources": [], "detail": { "modifiedAt": "2020-06-24T22:54:57.161Z", "ResourceTypeOptInPreference": { "Aurora": true }, "state": "MODIFIED" } }</pre>

Diferenças com oAWS BackupAPI de notificação

Você também pode usar o[AWS BackupAPI de notificação](#) para acompanhar oAWS BackupCom o Amazon Simple Notification Service (Amazon SNS). No entanto, o EventBridge rastreia mais alterações do que a API de notificação, incluindo alterações em cofres de backup, estado do trabalho de cópia, configurações de região e o número de pontos de recuperação inativos ou quentes.

MonitoramentoAWS Backupmétricas com o CloudWatch

Tópicos

- [Monitore métricas com o CloudWatch](#) (p. 191)
- [Diferenças com oAWS Backuppainel](#) (p. 193)

Monitore métricas com o CloudWatch

Você pode usar o CloudWatch para monitorarAWS BackupMétricas do . OBackupO namespace permite que você acompanhe as métricas a seguir.AWS BackupO emite métricas atualizadas para o CloudWatch a cada 5 minutos.

O objetivo desta página de documentação é fornecer a você os materiais de referência para usar o CloudWatch para monitorarAWS Backup. Para saber como monitorar uma métrica usando o CloudWatch, consulte o blog[Amazon CloudWatch Events e métricas para oAWS Backup](#)ou[Concentrar métricas e alarmes em um únicoAWSServiço](#)noGuia do usuário do CloudWatch. Para definir alarmes, consulte[Uso de alarmes do Amazon CloudWatch](#)noGuia do usuário do CloudWatch.

Categoria	Métricas	Exemplos de dimensões	Exemplo de caso de uso
Trabalhos	Número de trabalhos de backup, restauração e cópia em cada estado, incluindoCREATED,PENDING,REMOVING,ABORTED,COMPLETEDeEXPIRED. 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 trabalhos de backup com falha em um ou mais cofres de backup específicos. Quando houver mais de cinco trabalhos com falha em 1 hora, envie um e-mail ou SMS usando o Amazon SNS ou abra um tíquete para a equipe de engenharia para investigar. Critérios do: Há um valor diferente de zero
Pontos de recuperação	Número de pontos de recuperação quentes e frios em cada estado:MODIFIED,COMPLETED,PARTIAL,EXPIRED,Deleted	Tipo de recurso, nome do cofre.	Rastreie o número de pontos de recuperação excluídos para seus volumes do Amazon EBS e rastreie separadamente o número de pontos de recuperação quentes e frios em cada cofre de backup. Critérios do: Há um valor diferente de zero

A tabela a seguir lista todas as métricas disponíveis para você.

Métrica	Descrição
NumberOfBackupJobsCreated	O número de tarefas de backup que oAWS Backupcriado.
NumberOfBackupJobsPending	O número de trabalhos de backup prestes a ser executados noAWS Backup.
NumberOfBackupJobsRunning	O número de trabalhos de backup atualmente em execução noAWS Backup.
NumberOfBackupJobsAborted	O número de trabalhos de backup cancelados pelo usuário.
NumberOfBackupJobsCompleted	O número de tarefas de backup que oAWS BackupTerminada.
NumberOfBackupJobsFailed	O número de tarefas de backup que oAWS Backupagendado, mas não foi iniciado. Muitas vezes causado pelo agendamento de um trabalho de backup durante ou 4 horas antes da janela de manutenção de um recurso de banco de dados ou da janela de backup automatizado.AWS Backupnão executará seu trabalho agendado para manter sua integridade de dados.
NumberOfBackupJobsExpired	O número de tarefas de backup que oAWS Backuptentou excluir com base no ciclo de vida de retenção do backup, mas não foi possível excluir. Você será cobrado pelo armazenamento consumido pelos backups expirados e deve excluí-los manualmente.
NumberOfCopyJobsCreated	O número de trabalhos de cópia entre contas e regiões queAWS Backupcriado.
NumberOfCopyJobsRunning	O número de trabalhos de cópia entre contas e regiões em execução noAWS Backup.
NumberOfCopyJobsCompleted	O número de trabalhos de cópia entre contas e regiões queAWS BackupTerminada.
NumberOfCopyJobsFailed	O número de trabalhos de cópia entre contas e regiões queAWS Backuptentou, mas não foi possível concluir.
NumberOfRestoreJobsPending	O número de trabalhos de restauração prestes a ser executados noAWS Backup.
NumberOfRestoreJobsRunning	O número de trabalhos de restauração atualmente em execução noAWS Backup.
NumberOfRestoreJobsCompleted	O número de tarefas de restauração que oAWS BackupTerminada.
NumberOfRestoreJobsFailed	O número de tarefas de restauração que oAWS Backuptentou, mas não foi possível concluir.

Métrica	Descrição
NumberOfRecoveryPointsCompleted	O número de pontos de recuperação queAWS Backupcriado.
NumberOfRecoveryPointsPartial	O número de pontos de recuperação queAWS Backupcomeçou a criar, mas não conseguiu terminar.AWS tenta novamente o processo mais tarde, mas como a repetição ocorre posteriormente, ele mantém o ponto de recuperação parcial.
NumberOfRecoveryPointsExpired	O número de pontos de recuperação queAWS Backup tentou excluir com base no ciclo de vida de retenção do backup, mas não foi possível excluir. Você será cobrado pelo armazenamento consumido pelos backups expirados e deve excluí-los manualmente.
NumberOfRecoveryPointsDeleting	O número de pontos de recuperação queAWS Backupestá excluindo.
NumberOfRecoveryPointsCold	O número de pontos de recuperação queAWS BackupConceitos em camadas do armazenamento a frio.

Mais dimensões estão disponíveis além das listadas na tabela. Para exibir todas as dimensões de uma métrica, digite o nome dessa métrica na caixaBackupO namespace doMétricasdo console do CloudWatch.

Diferenças com oAWS Backuppainel

OAWS Backuptem seu próprio painel, que você pode visualizar escolhendoPainelNo painel de navegação. Este painel mostra métricas para as últimas 24 horas. O painel do CloudWatch mostra métricas durante um período de tempo mais longo. Para obter detalhes, consulte[Qual é o período de retenção de todas as métricas?](#)noPerguntas frequentes sobre CloudWatch.

OAWS Backup também mostra métricas em um ponto no tempo. O CloudWatch mostra métricas por um período. Por exemplo, suponha que você tenha nove trabalhos concluídos e um trabalho em andamento nas últimas 4 horas. OAWS Backupmostraria nove trabalhos concluídos e um trabalho em andamento. O CloudWatch mostraria 10 trabalhos em andamento se você visualizar métricas de tarefas em execução nas últimas 4 horas.

Recomendamos que você use o painel do que permite detectar problemas em potencial com mais facilidade.

Registro em logAWS BackupChamadas de API com CloudTrail

O AWS Backup é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no AWS Backup. O CloudTrail captura todas as chamadas de API para oAWS Backupcomo eventos. As chamadas capturadas incluem as chamadas do console do AWS Backup e as chamadas de código para as operações da API do AWS Backup. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail a um bucket do Amazon

S3, incluindo eventos para oAWS Backup. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o AWS Backup, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais. Para saber mais sobre o CloudTrail, consulte o [Manual do usuário do AWS CloudTrail](#).

Tópicos

- [AWS BackupInformações do no CloudTrail \(p. 194\)](#)
- [Noções básicas sobre entradas de arquivos de log do AWS Backup \(p. 195\)](#)
- [Registrar em log eventos de gerenciamento \(p. 197\)](#)

AWS BackupInformações do no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando a atividade ocorre emAWS Backup, essa atividade é registrada em um evento do CloudTrail junto com outrosAWSEventos de serviço noHistórico do evento. Você pode visualizar, pesquisar e fazer download de eventos recentes em seuAWSconta.AWS Backupgera estes eventos do CloudTrail quando ele executa backups, restaurações, cópias ou notificações:

- BackupDeleted
- BackupJobCompleted
- BackupJobStarted
- BackupSelectionDeletedDueToSLRDeletion
- BackupTransitionedToCold
- CopyJobCompleted
- CopyJobStarted
- RestoreCompleted
- RestoreStarted
- PutBackupVaultNotifications

Esses eventos não são necessariamente gerados pelo uso doAWS BackupAPIs públicas. Em vez disso, eles são gerados atravésAWS Backupexecução assíncrona de seus trabalhos. Por exemplo, seuStartBackupJobchamada de API pode gerar oBackupJobStarted, mas um trabalho agendado de um plano de backup também pode gerar o eventoBackupJobStartedEvento .

Para mais informações, consulte [Visualizar eventos com o histórico de eventos do CloudTrail](#).

Para obter um registro contínuo de eventos na conta da AWS, incluindo eventos do AWS Backup, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros serviços da AWS para analisar mais profundamente e agir sobre os dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços e integrações compatíveis com o CloudTrail](#)
- [Configuração de notificações do Amazon SNS para o CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas](#)

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 do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o [Elemento `userIdentity` do CloudTrail](#).

Noções básicas sobre entradas de arquivos de log do AWS Backup

Uma trilha é uma configuração que permite a entrega de eventos como registros de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra `oStartBackupJob`, `StartRestoreJob`, `eDeleteRecoveryPoint` também `oBackupJobCompletedEvent`.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "account-id",
    "accessKeyId": "access-key",
    "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": "account-id",
    "accessKeyId": "access-key",
    "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": "783ddddd-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": "account-id",
    "accessKeyId": "access-key",
    "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": "account-id",
    "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

O uso do AWS Backup, é possível gerenciar os backups em todos os AWS Contas no [AWS Organizations](#) Estrutura. AWS Backup O gera esses eventos do CloudTrail ao criar, atualizar ou excluir um AWS Organizations política de backup (que aplica planos de backup às suas contas de membro):

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`

Exemplo: AWS Backup Entradas de arquivo de log para gerenciamento entre contas

Uma trilha é uma configuração que permite a entrega de eventos como registros de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `CreateOrganizationalBackupPlan`.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "account-id",
    "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": "account-id"
    }
  }
}
```

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `DeleteOrganizationalBackupPlan`.

```
{
```

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "account-id",
    "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": "account-id"
  }
}
```

Usando o Amazon SNS para rastrear AWS Backup eventos

AWS Backup O aproveita as notificações robustas fornecidas pelo Amazon Simple Notification Service (Amazon SNS). Você pode configurar o Amazon SNS para notificá-lo sobre o AWS Backup no console do Amazon SNS.

Tópicos

- [Configurando o console do Amazon SNS \(p. 199\)](#)
- [AWS Backup APIs de notificação \(p. 200\)](#)
- [Exemplos de eventos \(p. 200\)](#)
- [AWS Backup Exemplos de comandos de \(p. 202\)](#)
- [Especificando AWS Backup Como um principal de serviço \(p. 203\)](#)

Configurando o console do Amazon SNS

Para obter um tutorial sobre como configurar o console do Amazon SNS para enviar AWS Backup notificações relacionadas ao, siga as etapas em [Como posso obter notificações do para o AWS Backup trabalhos que falharam?](#) from AWS Premium Support.

Para obter mais informações, 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 o seguinte AWS Backup Operações de API para gerenciar suas notificações de backup.

- [DeleteBackupVaultNotifications](#) (p. 228)— Excluir notificações de eventos para o cofre de backup especificado.
- [GetBackupVaultNotifications](#) (p. 276)— Lista as notificações de eventos para o cofre de backup especificado.
- [PutBackupVaultNotifications](#) (p. 319) Ativa as notificações para o tópico e os eventos especificados.

Os seguintes eventos são compatíveis:

Tipo de trabalho	Evento
Trabalho de backup	BACKUP_JOB_STARTED BACKUP_JOB_COMPLETED
Copiar trabalho	COPY_JOB_STARTED COPY_JOB_SUCCESSFUL COPY_JOB_FAILED
Trabalhos de restauração	RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
Ponto de recuperação	RECOVERY_POINT_MODIFIED

Exemplos de eventos

Evento	Notificações do Amazon SNS
Trabalho de backup concluído	<pre>{ "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",</pre>

Evento	Notificações do Amazon SNS
	<pre> ... "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" } } } } </pre>
Falha no trabalho de backup	<pre> { "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" } } }] } </pre>

Evento	Notificações do Amazon SNS
O trabalho de backup não pôde ser concluído durante a janela de backup	<pre>{ "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" } } }] }</pre>

AWS BackupExemplos de comandos de

Você pode usarAWS CLIPara se inscrever, listar e excluir notificações do Amazon SNS para o seuAWS Backup.

Exemplo de notificação put backup vault

O comando a seguir faz a inscrição em um tópico do Amazon SNS para o cofre de backup especificado que avisa 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 --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
--backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED RECOVERY_POINT_MODIFIED
```


Exemplo de obter notificação do 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 notificação de exclusão de segurança

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
```

EspecificandoAWS BackupComo um principal de serviço

Note

Para permitir a que o AWS Backup publique tópicos do SNS em seu nome, você deve especificar o AWS Backup como um principal de serviço.

Inclua o seguinte JSON na política de acesso do tópico do Amazon SNS que você usa para rastrearAWS Backup. 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"
}
```

O JSON de exemplo a seguir mostra uma política de acesso básica do Amazon SNS que inclui oAWS Backupcomo um diretor de serviço. Este exemplo permite o acesso entre contas.

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
```

```
"Statement": [
  {
    "Sid": "__default_statement_ID",
    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": [
      "SNS:Publish",
      "SNS:RemovePermission",
      "SNS:SetTopicAttributes",
      "SNS>DeleteTopic",
      "SNS:ListSubscriptionsByTopic",
      "SNS:GetTopicAttributes",
      "SNS:Receive",
      "SNS:AddPermission",
      "SNS:Subscribe"
    ],
    "Resource": "arn:aws:sns:region:account-id:myTopic",
    "Condition": {
      "StringEquals": {
        "AWS:SourceOwner": "account-id"
      }
    }
  },
  {
    "Sid": "__console_pub_0",
    "Effect": "Allow",
    "Principal": {
      "Service": "backup.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:region:account-id:myTopic"
  }
]
```

Para obter mais informações sobre como especificar um principal de serviço em uma política de acesso do Amazon SNS, consulte [Permitindo QualquerAWSRecurso a publicar em um tópico](#) no Guia do desenvolvedor do Amazon Simple Notification Service.

Note

Se o tópico estiver criptografado, você deverá incluir permissões adicionais em sua política para permitir que o AWS Backup publique nele. Para obter mais informações sobre como habilitar serviços para publicar em tópicos criptografados, consulte [Habilitar a compatibilidade entre fontes de eventos do AWS](#) no Guia do desenvolvedor do Amazon Simple Notification Service.

Solução de problemas do AWS Backup

Ao usar o AWS Backup, você pode encontrar problemas ao trabalhar com planos de backup, recursos e cofres de backup. As seções a seguir podem ajudar a solucionar alguns problemas comuns que podem ocorrer.

Em caso de perguntas gerais sobre o AWS Backup, consulte as [Perguntas frequentes sobre o AWS Backup](#). Você também pode procurar respostas e postar dúvidas no [Fórum do AWS Backup](#).

Tópicos

- [Solução de problemas gerais \(p. 205\)](#)
- [Solução de problemas de criação \(p. 205\)](#)
- [Solução de problemas de exclusão \(p. 206\)](#)

Solução de problemas gerais

Ao fazer backup e restaurar recursos, você não só precisa de permissão para usar o AWS Backup, mas também deve ter permissão para acessar os recursos que deseja proteger. Para obter mais informações sobre controle de acesso usando o AWS Identity and Access Management (IAM) AWS Backup, consulte [Controle de acesso \(p. 99\)](#).

Se tiver problemas com o backup e a restauração de um determinado tipo de recurso, pode ser útil rever o tópico de solução de problemas para esse recurso. Para obter mais informações sobre como solucionar problemas de outros AWS, consulte o seguinte:

- [O uso do AWS Backup com Amazon EFS](#) no Guia do usuário do Amazon Elastic File System
- [Backup e restauração sob demanda para o DynamoDB](#) no Guia do desenvolvedor do Amazon DynamoDB
- [Snapshots do Amazon EBS](#) no Guia do usuário do Amazon EC2 para instâncias do Linux
- [Backup e restauração de instâncias de banco de dados do Amazon RDS](#) no Guia do usuário do Amazon RDS
- [Visão geral do backup e da restauração de um cluster de banco de dados do Aurora](#) no Guia do usuário do Amazon Aurora.
- [Fazer backup de seus volumes](#) no Guia do usuário da AWS Storage Gateway

Se o AWS Backup falhar ao criar ou excluir um recurso, saiba mais sobre o problema usando o AWS CloudTrail para exibir mensagens de erro ou logs. Para obter mais informações sobre como usar o CloudTrail com AWS Backup, consulte [Registro em log AWS Backup Chamadas de API com CloudTrail \(p. 193\)](#).

Solução de problemas de criação

As informações a seguir podem ajudá-lo a solucionar problemas ao criar backups.

- A criação de backups para tabelas do DynamoDB falhará 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 7 dias quando os sistemas de arquivos são muito grandes. Para um sistema de arquivos do Amazon EFS, somente é possível colocar um backup simultâneo de cada vez na fila. 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 por AWS Região por conta. Quando essa cota é atingida, os backups adicionais falham. 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 RDS, considere o seguinte:
 - Se você não usar AWS Backup para gerenciar snapshots do Amazon RDS e backups contínuos com recuperação point-in-time, seus backups falharão se forem iniciados se agendados ou feitos sob demanda durante a janela diária de backup 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 snapshots do Amazon RDS e backups contínuos com a recuperação point-in-time.
 - 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.
 - Os backups iniciados durante uma janela de manutenção não irão funcionar. Para obter mais informações sobre janelas de manutenção do Amazon RDS, consulte [Manutenção de uma instância de banco de dados](#) no Guia do usuário do Amazon RDS.
 - Não é possível especificar opções do RDS ao usar AWS Backup para fazer uma cópia de backup. Se você receber um erro como `"The snapshot requires a target option group with the following options: Timezone..."`, é necessário remover a opção ou usar o console do Amazon RDS ou a API para iniciar a cópia.

Solução de problemas de exclusão

Os pontos de recuperação criados pelo AWS Backup não podem ser excluídos na janela de console do recurso protegido. Eles podem ser excluídos no console do AWS Backup selecionando-os no cofre onde 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 controle de acesso usando o IAM com AWS Backup, consulte [Controle de acesso](#) (p. 99).

API do AWS Backup

Além de usar o console do, você pode usar o AWS Backup Ações de API e tipos de dados para configurar e gerenciar programaticamente AWS Backup e seus recursos. Esta seção descreve AWS Backup ações e tipos de dados. Ele contém a referência da API do AWS Backup.

- [Ações](#)
- [Tipos de dados](#)
- [Erros comuns](#)

Actions

As ações a seguir são compatíveis:

- [CreateBackupPlan](#) (p. 209)
- [CreateBackupSelection](#) (p. 213)
- [CreateBackupVault](#) (p. 216)
- [DeleteBackupPlan](#) (p. 219)
- [DeleteBackupSelection](#) (p. 222)
- [DeleteBackupVault](#) (p. 224)
- [DeleteBackupVaultAccessPolicy](#) (p. 226)
- [DeleteBackupVaultNotifications](#) (p. 228)
- [DeleteRecoveryPoint](#) (p. 230)
- [DescribeBackupJob](#) (p. 232)
- [DescribeBackupVault](#) (p. 237)
- [DescribeCopyJob](#) (p. 240)
- [DescribeGlobalSettings](#) (p. 242)
- [DescribeProtectedResource](#) (p. 244)
- [DescribeRecoveryPoint](#) (p. 246)
- [DescribeRegionSettings](#) (p. 251)
- [DescribeRestoreJob](#) (p. 253)
- [DisassociateRecoveryPoint](#) (p. 257)
- [ExportBackupPlanTemplate](#) (p. 259)
- [GetBackupPlan](#) (p. 261)
- [GetBackupPlanFromJSON](#) (p. 265)
- [GetBackupPlanFromTemplate](#) (p. 268)
- [GetBackupSelection](#) (p. 271)
- [GetBackupVaultAccessPolicy](#) (p. 274)
- [GetBackupVaultNotifications](#) (p. 276)
- [GetRecoveryPointRestoreMetadata](#) (p. 279)
- [GetSupportedResourceTypes](#) (p. 282)
- [ListBackupJobs](#) (p. 284)
- [ListBackupPlans](#) (p. 287)
- [ListBackupPlanTemplates](#) (p. 290)

- [ListBackupPlanVersions](#) (p. 292)
- [ListBackupSelections](#) (p. 295)
- [ListBackupVaults](#) (p. 298)
- [ListCopyJobs](#) (p. 300)
- [ListProtectedResources](#) (p. 303)
- [ListRecoveryPointsByBackupVault](#) (p. 305)
- [ListRecoveryPointsByResource](#) (p. 308)
- [ListRestoreJobs](#) (p. 311)
- [ListTags](#) (p. 314)
- [PutBackupVaultAccessPolicy](#) (p. 317)
- [PutBackupVaultNotifications](#) (p. 319)
- [StartBackupJob](#) (p. 322)
- [StartCopyJob](#) (p. 326)
- [StartRestoreJob](#) (p. 330)
- [StopBackupJob](#) (p. 333)
- [TagResource](#) (p. 335)
- [UntagResource](#) (p. 337)
- [UpdateBackupPlan](#) (p. 339)
- [UpdateGlobalSettings](#) (p. 343)
- [UpdateRecoveryPointLifecycle](#) (p. 345)
- [UpdateRegionSettings](#) (p. 349)

CreateBackupPlan

Cria um plano de backup usando um nome de plano de backup e regras de backup. Um plano de backup é um documento que contém informações que AWS Backup usa para agendar tarefas que criam pontos de recuperação para recursos.

Se você chamar `CreateBackupPlan` com um plano que já existe, um `AlreadyExistsException` é retornado.

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
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "Lifecycle": {
          "DeleteAfterDays": number,
          "MoveToColdStorageAfterDays": number
        },
        "RecoveryPointTags": {
          "string": "string"
        },
        "RuleName": "string",
        "ScheduleExpression": "string",
        "StartWindowMinutes": number,
        "TargetBackupVaultName": "string"
      }
    ]
  },
  "BackupPlanTags": {
    "string": "string"
  },
  "CreatorRequestId": "string"
}
```

Parâmetros da solicitação

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

BackupPlan (p. 209)

Especifica o corpo de um plano de backup. Inclui um `BackupPlanName` e um ou mais conjuntos de `Rules`.

Tipo: objeto [BackupPlanInput](#) (p. 359)

: obrigatório Sim

BackupPlanTags (p. 209)

Para ajudar a organizar seus recursos, você pode atribuir seus próprios metadados aos recursos que criar. Cada tag é um par de chave-valor. As tags especificadas são atribuídas a todos os backups criados com esse plano.

Type: Mapa de string para string

: obrigatório Não

CreatorRequestId (p. 209)

Identifica a solicitação e permite que 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 é retornado. Esse parâmetro é opcional.

Type: String

: 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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[AdvancedBackupSettings \(p. 210\)](#)

Lista de `BackupOptions` As configurações de um tipo de recurso. Essa opção só está disponível para trabalhos de backup do Windows VSS.

Type: Array [AdvancedBackupSetting \(p. 352\)](#) objects

[BackupPlanArn \(p. 210\)](#)

Um nome de 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`.

Type: String

[BackupPlanId \(p. 210\)](#)

Identifica exclusivamente um plano de backup.

Type: String

[CreationDate \(p. 210\)](#)

A data e hora em que um plano de backup é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[VersionId \(p. 210\)](#)

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. Eles não podem ser editados.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`AlreadyExistsException`

O recurso necessário já existe.

Código de status HTTP: 400

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`LimitExceededException`

Um limite na solicitação foi excedido; por exemplo, um número máximo de itens permitidos em uma solicitação.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateBackupSelection

Cria um documento JSON que especifica um conjunto de recursos para atribuir a um plano de backup. Os recursos podem ser incluídos especificando padrões para um `ListOfTags` selecionado `Resources`.

Por exemplo, considere os seguintes padrões:

- `Resources: "arn:aws:ec2:region:account-id:volume/volume-id"`
- `ConditionKey: "department"`
`ConditionValue: "finance"`
`ConditionType: "StringEquals"`
- `ConditionKey: "importance"`
`ConditionValue: "critical"`
`ConditionType: "StringEquals"`

O uso desses padrões faria backup de todos os volumes do Amazon Elastic Block Store (Amazon EBS) que são marcados como `"department=finance"`, `"importance=critical"`, além de um volume EBS com o ID do volume especificado.

Recursos e condições são aditivos na medida em que todos os recursos que correspondem ao padrão são selecionados. Isso não deve ser confundido com um AND lógico, onde todas as condições devem corresponder. Os padrões de correspondência são logicamente colocados juntos usando o operador OR. Em outras palavras, todos os padrões correspondentes são selecionados para backup.

Sintaxe da solicitação

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
Content-type: application/json

{
  "BackupSelection": {
    "IamRoleArn": "string",
    "ListOfTags": [
      {
        "ConditionKey": "string",
        "ConditionType": "string",
        "ConditionValue": "string"
      }
    ],
    "Resources": [ "string" ],
    "SelectionName": "string"
  },
  "CreatorRequestId": "string"
}
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupPlanId](#) (p. 213)

Identifica exclusivamente o plano de backup a ser associado à seleção de recursos.

: obrigatório Sim

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[BackupSelection](#) (p. 213)

Especifica o corpo de uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Tipo: objeto [BackupSelection](#) (p. 367)

: obrigatório Sim

[CreatorRequestId](#) (p. 213)

Uma string exclusiva que identifica a solicitação e permite que solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes.

Type: String

: 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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupPlanId](#) (p. 214)

Identifica exclusivamente um plano de backup.

Type: String

[CreationDate](#) (p. 214)

A data e hora em que uma seleção de backup é criada, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[SelectionId](#) (p. 214)

Identifica exclusivamente o corpo de uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

AlreadyExistsException

O recurso necessário já existe.

Código de status HTTP: 400

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, um número máximo de itens permitidos em uma solicitação.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2 2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateBackupVault

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

Os dados confidenciais, como números de passaporte, não devem incluir o 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

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 216)

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 o AWSRegião onde foram criadas. Eles consistem em em em letras, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[BackupVaultTags](#) (p. 216)

Os metadados que você pode atribuir para ajudar a organizar os recursos que você criar. Cada tag é um par de chave-valor.

Type: Mapa de string para string

: obrigatório Não

[CreatorRequestId](#) (p. 216)

Uma string exclusiva que identifica a solicitação e permite que solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes.

Type: String

: obrigatório Não

EncryptionKeyArn (p. 216)

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`.

Type: String

: 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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

BackupVaultArn (p. 217)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

BackupVaultName (p. 217)

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 em que são criados. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

CreationDate (p. 217)

A data e hora em que um cofre de backup é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor `1516925490.087` representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

AlreadyExistsException

O recurso necessário já existe.

Código de status HTTP: 400

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`LimitExceededException`

Um limite na solicitação foi excedido; por exemplo, um número máximo de itens permitidos em uma solicitação.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupPlan

Exclui um plano de backup. Um plano de backup pode ser excluído somente depois que todas as seleções de recursos associadas forem excluídas. Excluir um plano de backup exclui a versão atual de um plano de backup. Versões anteriores, se houver, ainda existirão.

Sintaxe da solicitação

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupPlanId](#) (p. 219)

Identifica exclusivamente um plano de backup.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupPlanArn](#) (p. 219)

Um nome de 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`.

Type: String

[BackupPlanId](#) (p. 219)

Identifica exclusivamente um plano de backup.

Type: String

[DeletionDate \(p. 219\)](#)

A data e hora em que um plano de backup é excluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `DeletionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[VersionId \(p. 219\)](#)

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. IDs de versão não podem ser editados.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`InvalidRequestException`

indica que algo está errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)

- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupSelection

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

A solicitação usa os seguintes parâmetros de URI.

[BackupPlanId](#) (p. 222)

Identifica exclusivamente um plano de backup.

: obrigatório Sim

[SelectionId](#) (p. 222)

Identifica exclusivamente o corpo de uma solicitação para atribuir um conjunto de recursos a um plano de backup.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupVault

Exclui o cofre de backup identificado por seu nome. Um cofre só pode ser excluído se ele estiver vazio.

Sintaxe da solicitação

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

BackupVaultName (p. 224)

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 oAWSRegião onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

InvalidRequestException

indica que algo está errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupVaultAccessPolicy

Exclui o documento de política que gerencia permissões em um cofre de backup.

Sintaxe da solicitação

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 226)

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 o `AWSRegião` onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteBackupVaultNotifications

Excluir notificações de eventos para o cofre de backup especificado.

Sintaxe da solicitação

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 228)

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 em que são criados. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteRecoveryPoint

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 ponto de extremidade exclui o backup contínuo existente e interrompe o backup contínuo futuro.

Sintaxe da solicitação

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 230)

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 oAWSRegião onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

[RecoveryPointArn](#) (p. 230)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente 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 não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte[Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

InvalidRequestException

indica que algo está errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de status HTTP: 400

InvalidResourceException

AWS Backup já está executando uma ação nesse ponto de recuperação. Ele não pode executar a ação solicitada até que a primeira ação seja concluída. Tente novamente mais tarde.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeBackupJob

Retorna detalhes do trabalho de backup para oBackupJobId.

Sintaxe da solicitação

```
GET /backup-jobs/backupJobId HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupJobID](#) (p. 232)

Identificar exclusivamente uma solicitação paraAWS Backuppara fazer backup de um recurso.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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,
  "CompletionDate": number,
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanVersion": "string",
    "BackupRuleId": "string"
  },
  "CreationDate": number,
  "ExpectedCompletionDate": number,
  "IamRoleArn": "string",
  "PercentDone": "string",
  "RecoveryPointArn": "string",
  "ResourceArn": "string",
  "ResourceType": "string",
  "StartBy": number,
  "State": "string",
  "StatusMessage": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[AccountId \(p. 232\)](#)

Retorna o ID da conta que possui o trabalho de backup.

Type: String

Padrão: `^[0-9]{12}$`

[BackupJobID \(p. 232\)](#)

Identificar exclusivamente uma solicitação para AWS Backup para fazer backup de um recurso.

Type: String

[BackupOptions \(p. 232\)](#)

Representa as opções especificadas como parte do plano de backup ou da tarefa de backup sob demanda.

Type: Mapa de string para string

Pattern: `^[a-zA-Z0-9\-_\.\]{1,50}$`

Pattern: `^[a-zA-Z0-9\-_\.\]{1,50}$`

[BackupSizeInBytes \(p. 232\)](#)

O tamanho, em bytes, de um backup.

Type: Long

[BackupType \(p. 232\)](#)

Representa o tipo de backup real selecionado para um trabalho de backup. Por exemplo, se um backup WindowSVSS bem-sucedido foi feito, `BackupType` retorna "WindowsVSS". Se `BackupType` estiver vazio, então o tipo de backup que foi é um backup regular.

Type: String

[BackupVaultArn \(p. 232\)](#)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

[BackupVaultName \(p. 232\)](#)

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 o `AWSRegião` onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

[BytesTransferred \(p. 232\)](#)

O tamanho em bytes transferidos para um cofre de backup no momento em que o status do trabalho foi consultado.

Type: Long

[CompletionDate \(p. 232\)](#)

A data e hora em que um trabalho para criar um trabalho de backup é concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[CreatedBy \(p. 232\)](#)

Contém informações de identificação sobre a criação de um trabalho de backup, incluindo `oBackupPlanArn`, `BackupPlanId`, `BackupPlanVersion`, `eBackupRuleId` do plano de backup que é usado para criá-lo.

Tipo: objeto [RecoveryPointCreator \(p. 385\)](#)

[CreationDate \(p. 232\)](#)

A data e hora em que um trabalho de backup é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[ExpectedCompletionDate \(p. 232\)](#)

A data e hora em que um trabalho para fazer backup de recursos deve ser concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `ExpectedCompletionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[IamRoleArn \(p. 232\)](#)

Especifica o ARN da função do IAM usado para criar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

[Percentdone \(p. 232\)](#)

Contém uma porcentagem estimada que está concluída de um trabalho no momento em que o status do job foi consultado.

Type: String

[RecoveryPointArn \(p. 232\)](#)

Um ARN que identifica exclusivamente um ponto de recuperação; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

[ResourceArn \(p. 232\)](#)

Um ARN que identifica exclusivamente um recurso salvo. O formato do ARN depende do tipo de recurso.

Type: String

[ResourceType \(p. 232\)](#)

O tipo de `AWS` Um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

[StartBy \(p. 232\)](#)

Especifica a hora no formato Unix e Tempo Universal Coordenado (UTC) em que um trabalho de backup deve ser iniciado para ser cancelado. O valor é calculado adicionando a janela inicial à hora programada. Portanto, se o horário agendado fosse 18:00 PM e a janela de início for de 2 horas, o `startBy` seria 20h na data especificada. O valor de `startBy` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[Estado \(p. 232\)](#)

O estado atual de um ponto de recuperação de recursos.

Type: String

Valores válidos: `CREATED` | `PENDING` | `RUNNING` | `ABORTING` | `ABORTED` | `COMPLETED` | `FAILED` | `EXPIRED`

[StatusMessage \(p. 232\)](#)

Uma mensagem detalhada explicando o status do trabalho para fazer backup de um recurso.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`DependencyFailureException`

Dependente AWS serviço ou recurso retornou um erro para o AWS Backup e a ação não pode ser concluída.

Código de status HTTP: 500

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeBackupVault

Retorna metadados sobre um cofre de backup especificado por seu nome.

Sintaxe da solicitação

```
GET /backup-vaults/backupVaultName HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 237)

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 o `AWSRegião` onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CreationDate": number,
  "CreatorRequestId": "string",
  "EncryptionKeyArn": "string",
  "NumberOfRecoveryPoints": number
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupVaultArn](#) (p. 237)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

[BackupVaultName](#) (p. 237)

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 em que são criados. Eles consistem em letras minúsculas, números e hifens.

Type: String

[CreationDate \(p. 237\)](#)

A data e hora em que um cofre de backup é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[CreatorRequestId \(p. 237\)](#)

Uma string exclusiva que identifica a solicitação e permite que solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes.

Type: String

[EncryptionKeyArn \(p. 237\)](#)

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`.

Type: String

[Número de Pontos de Recuperação \(p. 237\)](#)

O número de pontos de recuperação que são armazenados em um cofre de backup.

Type: Long

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeCopyJob

Retorna metadados associados à criação de uma cópia de um recurso.

Sintaxe da solicitação

```
GET /copy-jobs/copyJobId HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[CopyJobID](#) (p. 240)

Identificar exclusivamente um trabalho de cópia.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "CopyJob": {
    "AccountId": "string",
    "BackupSizeInBytes": number,
    "CompletionDate": number,
    "CopyJobId": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
    },
    "CreationDate": number,
    "DestinationBackupVaultArn": "string",
    "DestinationRecoveryPointArn": "string",
    "IamRoleArn": "string",
    "ResourceArn": "string",
    "ResourceType": "string",
    "SourceBackupVaultArn": "string",
    "SourceRecoveryPointArn": "string",
    "State": "string",
    "StatusMessage": "string"
  }
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[CopyJob \(p. 240\)](#)

Contém informações detalhadas sobre um trabalho de cópia.

Tipo: objeto [CopyJob \(p. 375\)](#)

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeGlobalSettings

Descreve se o AWS tem optado por fazer backup entre contas. Retorna um erro se a conta não for membro de uma organização de Organizations. Exemplo: `describe-global-settings --region us-west-2`

Sintaxe da solicitação

```
GET /global-settings HTTP/1.1
```

Parâmetros da solicitação

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[globalSettings](#) (p. 242)

O status da bandeira `isCrossAccountBackupEnabled`.

Type: Mapa de string para string

[LastUpdateTime](#) (p. 242)

A data e a hora da sinalização `isCrossAccountBackupEnabled` foi atualizado pela última vez. Esta atualização está em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastUpdateTime` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

InvalidRequestException

indica que algo está errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeProtectedResource

Retorna informações sobre um recurso salvo, incluindo a última vez em que foi feito o backup, o Nome de recurso da Amazon (ARN) e o AWS do recurso salvo.

Sintaxe da solicitação

```
GET /resources/resourceArn HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[resourceArn](#) (p. 244)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um recurso. O formato do ARN depende do tipo de recurso.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "LastBackupTime": number,
  "ResourceArn": "string",
  "ResourceType": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[LastBackupTime](#) (p. 244)

A data e hora em que um recurso foi copiado pela última vez, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastBackupTime` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[ResourceArn](#) (p. 244)

Um ARN que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

Type: String

ResourceType (p. 244)

O tipo deAWSsalvo como um ponto de recuperação; por exemplo, um volume do EBS ou um banco de dados do Amazon RDS.

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte[Erros comuns](#) (p. 388).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeRecoveryPoint

Retorna metadados associados a um ponto de recuperação, incluindo ID, status, criptografia e ciclo de vida.

Sintaxe da solicitação

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 246)

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 oAWSRegião onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

[RecoveryPointArn](#) (p. 246)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente 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 não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupSizeInBytes": number,
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CalculatedLifecycle": {
    "DeleteAt": number,
    "MoveToColdStorageAt": number
  },
  "CompletionDate": number,
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanVersion": "string",
    "BackupRuleId": "string"
  },
  "CreationDate": number,
  "EncryptionKeyArn": "string",
```

```
"IamRoleArn": "string",
"IsEncrypted": boolean,
"LastRestoreTime": number,
"Lifecycle": {
  "DeleteAfterDays": number,
  "MoveToColdStorageAfterDays": number
},
"RecoveryPointArn": "string",
"ResourceArn": "string",
"ResourceType": "string",
"SourceBackupVaultArn": "string",
"Status": "string",
"StorageClass": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupSizeInBytes \(p. 246\)](#)

O tamanho, em bytes, de um backup.

Type: Long

[BackupVaultArn \(p. 246\)](#)

Um ARN que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

[BackupVaultName \(p. 246\)](#)

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 em que são criados. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

[Ciclo de vida calculado \(p. 246\)](#)

A `CalculatedLifecycle` objeto contendo `DeleteAt` e `MoveToColdStorageAt` timestamps.

Tipo: objeto [CalculatedLifecycle \(p. 372\)](#)

[CompletionDate \(p. 246\)](#)

A data e hora em que um trabalho para criar um ponto de recuperação é concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[CreatedBy \(p. 246\)](#)

Contém informações de identificação sobre a criação de um ponto de recuperação, incluindo o `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion`, e `BackupRuleId` do plano de backup usado para criá-lo.

Tipo: objeto [RecoveryPointCreator](#) (p. 385)

[CreationDate](#) (p. 246)

A data e hora em que um ponto de recuperação é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `creationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[EncryptionKeyArn](#) (p. 246)

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`.

Type: String

[IamRoleArn](#) (p. 246)

Especifica o ARN da função do IAM usado para criar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

[IsEncrypted](#) (p. 246)

Um valor Booleano retornado como `TRUE` se o ponto de recuperação especificado estiver criptografado, ou `FALSE` se o ponto de recuperação não estiver criptografado.

Type: Booleano

[LastRestoreTime](#) (p. 246)

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` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[Ciclo de vida](#) (p. 246)

O ciclo de vida define quando um recurso protegido é passado para armazenamento de baixa atividade e quando expira. AWS Backup faz com que os backups sejam transferidos e expirados 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 "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio".

Tipo: objeto [Lifecycle](#) (p. 378)

[RecoveryPointArn](#) (p. 246)

Um ARN que identifica exclusivamente um ponto de recuperação; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

[ResourceArn \(p. 246\)](#)

Um ARN que identifica exclusivamente um recurso salvo. O formato do ARN depende do tipo de recurso.

Type: String

[ResourceType \(p. 246\)](#)

O tipo de AWS recurso para salvar como um 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).

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

[sourceBackupVaultARN \(p. 246\)](#)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente o cofre de origem em que o recurso foi feito originalmente para backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:BackupVault`. Se a recuperação for restaurada para o mesmo AWS Região, este valor será `null`.

Type: String

[Status \(p. 246\)](#)

Um código de status especificando o estado do ponto de recuperação.

`PARTIAL` status indica AWS Backup não foi possível criar o ponto de recuperação antes da janela de backup ser fechada. Para aumentar a janela do 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` indica que o ponto de recuperação excedeu seu período de retenção, mas AWS Backup não tem permissão ou não é capaz de excluí-la. Para excluir manualmente esses pontos de recuperação, consulte [Etapa 3: Excluir os pontos de recuperação](#) no [Limpar os recursos](#) seção de Conceitos básicos.

Type: String

Valores válidos: `COMPLETED` | `PARTIAL` | `DELETING` | `EXPIRED`

[StorageClass \(p. 246\)](#)

Especifica a classe de armazenamento do ponto de recuperação. Os valores válidos são `WARM` ou `COLD`.

Type: String

Valores válidos: `WARM` | `COLD` | `DELETED`

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeRegionSettings

Retorna as configurações atuais de opção pelo serviço para a Região. Se o service-opt-in estiver habilitado para um serviço, AWS Backup tenta proteger os recursos desse serviço nesta região, quando o recurso está incluído em um backup sob demanda ou plano de backup agendado. Caso contrário, AWS Backup não tenta proteger os recursos desse serviço nesta Região, AWS Backup não tenta proteger os recursos desse serviço nesta Região.

Sintaxe da solicitação

```
GET /account-settings HTTP/1.1
```

Parâmetros da solicitação

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "ResourceTypeOptInPreference": {
    "string" : boolean
  }
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[ResourceTypeOptInPreference \(p. 251\)](#)

Retorna uma lista de todos os serviços junto com as preferências de opt-in na Região.

Type: Mapa de string para booleano

Pattern: `^[a-zA-Z0-9\-_\.\]{1,50}$`

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeRestoreJob

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

A solicitação usa os seguintes parâmetros de URI.

[RestoreJobId](#) (p. 253)

Identifica exclusivamente o trabalho que restaura um ponto de recuperação.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountId": "string",
  "BackupSizeInBytes": number,
  "CompletionDate": number,
  "CreatedResourceArn": "string",
  "CreationDate": number,
  "ExpectedCompletionTimeMinutes": number,
  "IamRoleArn": "string",
  "PercentDone": "string",
  "RecoveryPointArn": "string",
  "ResourceType": "string",
  "RestoreJobId": "string",
  "Status": "string",
  "StatusMessage": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[AccountId](#) (p. 253)

Retorna o ID da conta que possui o trabalho de restauração.

Type: String

Padrão: `^[0-9]{12}$`

[BackupSizeInBytes \(p. 253\)](#)

O tamanho, em bytes, do recurso retornado.

Type: Long

[CompletionDate \(p. 253\)](#)

A data e hora em que um trabalho para restaurar um ponto de recuperação é concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[CreatedResourceArn \(p. 253\)](#)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um recurso cujo ponto de recuperação está sendo restaurado. O formato do ARN depende do tipo de recurso do recurso de backup.

Type: String

[CreationDate \(p. 253\)](#)

A data e hora em que um trabalho de restauração é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[ExpectedCompletionTimeInNutes \(p. 253\)](#)

A quantidade de tempo em minutos que um trabalho restaurando um ponto de recuperação deve levar.

Type: Long

[IamRoleArn \(p. 253\)](#)

Especifica o ARN da função do IAM usado para criar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

[Percentdone \(p. 253\)](#)

Contém uma porcentagem estimada que está concluída de um trabalho no momento em que o status do job foi consultado.

Type: String

[RecoveryPointArn \(p. 253\)](#)

Um ARN que identifica exclusivamente um ponto de recuperação; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

[ResourceType \(p. 253\)](#)

Retorna metadados associados a um trabalho de restauração listado por tipo de recurso.

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

[RestoreJobid \(p. 253\)](#)

Identifica exclusivamente o trabalho que restaura um ponto de recuperação.

Type: String

[Status \(p. 253\)](#)

Código de status especificando o estado do job iniciado peloAWS BackupPara restaurar um ponto de recuperação.

Type: String

Valores válidos: `PENDING` | `RUNNING` | `COMPLETED` | `ABORTED` | `FAILED`

[StatusMessage \(p. 253\)](#)

Uma mensagem que mostra o status de um trabalho para restaurar um ponto de recuperação.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte[Erros comuns \(p. 388\)](#).

`DependencyFailureException`

DependenteAWSserviço ou recurso retornou um erro para oAWS Backupe a ação não pode ser concluída.

Código de status HTTP: 500

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)

- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DisassociateRecoveryPoint

Exclui o ponto de recuperação de backup contínuo especificado doAWS Backup e libera o controle desse backup contínuo para o serviço de origem, como o Amazon RDS. O serviço de origem continuará a criar e reter backups contínuos usando o ciclo de vida especificado no plano de backup original.

Não suporta pontos de recuperação de backup de instantâneos.

Sintaxe da solicitação

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 257)

O nome exclusivo de umAWS Backupcofre. Obrigatório.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

[RecoveryPointArn](#) (p. 257)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente umAWS BackupPonto de recuperação. Obrigatório.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte[Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

InvalidRequestException

indica que algo está errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de status HTTP: 400

InvalidResourceException

AWS Backup já está executando uma ação nesse ponto de recuperação. Ele não pode executar a ação solicitada até que a primeira ação seja concluída. Tente novamente mais tarde.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ExportBackupPlanTemplate

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

A solicitação usa os seguintes parâmetros de URI.

[BackupPlanId](#) (p. 259)

Identifica exclusivamente um plano de backup.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanTemplateJson": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupPlanTemplateJSON](#) (p. 259)

O corpo de um modelo de plano de backup no formato JSON.

Note

Este é um documento JSON assinado que não pode ser modificado antes de ser passado para `GetBackupPlanFromJSON`.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupPlan

Retorna BackupPlanDetalhes do especificado BackupPlanId. 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

A solicitação usa os seguintes parâmetros de URI.

[BackupPlanId](#) (p. 261)

Identifica exclusivamente um plano de backup.

: obrigatório Sim

[VersionId](#) (p. 261)

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

A solicitação não tem um corpo de solicitação.

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
        }
    ],
    "EnableContinuousBackup": boolean,
    "Lifecycle": {
        "DeleteAfterDays": number,
        "MoveToColdStorageAfterDays": number
    },
    "RecoveryPointTags": {
        "string" : "string"
    },
    "RuleId": "string",
    "RuleName": "string",
    "ScheduleExpression": "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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[AdvancedBackupSettings](#) (p. 261)

Contém uma lista de `BackupOptions` para cada tipo de recurso. A lista é preenchida somente se a opção avançada estiver definida para o plano de backup.

Type: Array [AdvancedBackupSetting](#) (p. 352) objects

[BackupPlan](#) (p. 261)

Especifica o corpo de um plano de backup. Inclui um `BackupPlanName` e um ou mais conjuntos de `Rules`.

Tipo: objeto [BackupPlan](#) (p. 358)

[BackupPlanArn](#) (p. 261)

Um nome de 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`.

Type: String

[BackupPlanId](#) (p. 261)

Identifica exclusivamente um plano de backup.

Type: String

[CreationDate \(p. 261\)](#)

A data e hora em que um plano de backup é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[CreatorRequestId \(p. 261\)](#)

Uma string exclusiva que identifica a solicitação e permite que solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes.

Type: String

[DeletionDate \(p. 261\)](#)

A data e hora em que um plano de backup é excluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `DeletionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[LastExecutionDate \(p. 261\)](#)

A última vez que um trabalho para fazer backup de recursos foi executado com este plano de backup. Uma data e hora, no formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastExecutionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[VersionId \(p. 261\)](#)

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. IDs de versão não podem ser editados.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupPlanFromJSON

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

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[BackupPlanTemplateJSON](#) (p. 265)

Um documento de plano de backup fornecido pelo cliente no formato JSON.

Type: 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
            }
          }
        ]
      }
    ],
    "EnableContinuousBackup": boolean,
  }
}
```

```
    "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number
    },
    "RecoveryPointTags": {
      "string" : "string"
    },
    "RuleId": "string",
    "RuleName": "string",
    "ScheduleExpression": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string"
  }
}
]
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupPlan \(p. 265\)](#)

Especifica o corpo de um plano de backup. Inclui um `BackupPlanName` e um ou mais conjuntos de `Rules`.

Tipo: objeto [BackupPlan \(p. 358\)](#)

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`InvalidRequestException`

indica que algo está 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, um número máximo de itens permitidos em uma solicitação.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupPlanFromTemplate

Retorna o modelo especificado pelo seu `templateId` como um plano de backup.

Sintaxe da solicitação

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[TemplateId](#) (p. 268)

Identifica exclusivamente um modelo de plano de backup armazenado.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "Lifecycle": {
          "DeleteAfterDays": number,
          "MoveToColdStorageAfterDays": number
        },
        "RecoveryPointTags": {
          "string": "string"
        }
      }
    ]
  }
}
```

```
    "RuleId": "string",  
    "RuleName": "string",  
    "ScheduleExpression": "string",  
    "StartWindowMinutes": number,  
    "TargetBackupVaultName": "string"  
  }  
]  
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupPlanDocument](#) (p. 268)

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](#) (p. 358)

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)

- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupSelection

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

A solicitação usa os seguintes parâmetros de URI.

[BackupPlanId](#) (p. 271)

Identifica exclusivamente um plano de backup.

: obrigatório Sim

[SelectionId](#) (p. 271)

Identifica exclusivamente o corpo de uma solicitação para atribuir um conjunto de recursos a um plano de backup.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanId": "string",
  "BackupSelection": {
    "IamRoleArn": "string",
    "ListOfTags": [
      {
        "ConditionKey": "string",
        "ConditionType": "string",
        "ConditionValue": "string"
      }
    ],
    "Resources": [ "string" ],
    "SelectionName": "string"
  },
  "CreationDate": number,
  "CreatorRequestId": "string",
  "SelectionId": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupPlanId \(p. 271\)](#)

Identifica exclusivamente um plano de backup.

Type: String

[BackupSelection \(p. 271\)](#)

Especifica o corpo de uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Tipo: objeto [BackupSelection \(p. 367\)](#)

[CreationDate \(p. 271\)](#)

A data e hora em que uma seleção de backup é criada, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `creationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[CreatorRequestId \(p. 271\)](#)

Uma string exclusiva que identifica a solicitação e permite que solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes.

Type: String

[SelectionId \(p. 271\)](#)

Identifica exclusivamente o corpo de uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupVaultAccessPolicy

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

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 274)

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 o `AWSRegião` onde foram criados. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupVaultArn](#) (p. 274)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

[BackupVaultName](#) (p. 274)

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 em que são criados. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

[Política \(p. 274\)](#)

O documento da política de acesso ao cofre de backup no formato JSON.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2 2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetBackupVaultNotifications

Retorna notificações de eventos para o cofre de backup especificado.

Sintaxe da solicitação

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 276)

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 oAWSRegião onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupVaultArn](#) (p. 276)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo,`arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

[BackupVaultEvents](#) (p. 276)

Uma matriz de eventos que indicam o status de trabalhos para recursos de backup para o cofre de backup.

Type: 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

[BackupVaultName \(p. 276\)](#)

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 em que são criados. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

[SNSTopicArn \(p. 276\)](#)

Um ARN que identifica exclusivamente um tópico do Amazon Simple Notification Service (Amazon SNS); por exemplo, `arn:aws:sns:us-west-2:111122223333:MyTopic`.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)

- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2 2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetRecoveryPointRestoreMetadata

Retorna um conjunto de pares de valores chave que foram usados para criar o backup.

Sintaxe da solicitação

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata
HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 279)

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 oAWSRegião onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_]{2,50}$`

: obrigatório Sim

[RecoveryPointArn](#) (p. 279)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente 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 não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "RecoveryPointArn": "string",
  "RestoreMetadata": {
    "string" : "string"
  }
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupVaultArn](#) (p. 279)

Um ARN que identifica exclusivamente um cofre de backup, por exemplo,`arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

[RecoveryPointArn](#) (p. 279)

Um ARN que identifica exclusivamente um ponto de recuperação; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

[RestoreMetadados](#) (p. 279)

O conjunto de pares chave-valor de metadados que descrevem a configuração original do recurso de backup. Esses valores variam dependendo do serviço que está sendo restaurado.

Type: Mapa de string para string

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2 2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

GetSupportedResourceTypes

Retorna oAWSTipos de recursos compatíveis com oAWS Backup.

Sintaxe da solicitação

```
GET /supported-resource-types HTTP/1.1
```

Parâmetros da solicitação

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "ResourceTypes": [ "string" ]
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[ResourceTypes \(p. 282\)](#)

Contém uma string com oAWSTipos de recursos do :

- `DynamoDB` para o Amazon DynamoDB
- `EBSAmazon` Elastic Block Store
- `EC2` para o Amazon Elastic Compute Cloud
- `EFS` para o Amazon Elastic File System
- `RDSAmazon` Relational Database Service
- `Aurora` para o Amazon Aurora
- `Storage Gateway` para AWS Storage Gateway

Type: Matriz de strings

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupJobs

Retorna uma lista de trabalhos de backup existentes para uma conta autenticada nos últimos 30 dias. Por um período de tempo mais longo, considere usar estes [Ferramentas de monitoramento](#).

Sintaxe da solicitação

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore
HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[PorAccountId](#) (p. 284)

O ID da conta a partir do qual listar os trabalhos. Retorna somente trabalhos de backup associados ao ID de conta especificado.

Se usado a partir de uma AWS Organizations conta de gerenciamento, passando * retorna todos os trabalhos em toda a organização.

Padrão: `^[0-9]{12}$`

[ByBackupVaultName](#) (p. 284)

Retorna apenas 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 o AWS Região onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

[byCreateDafter](#) (p. 284)

Retorna somente trabalhos de backup que foram criados após a data especificada.

[PorCreatedBefore](#) (p. 284)

Retorna somente trabalhos de backup que foram criados antes da data especificada.

[ByResourceArn](#) (p. 284)

Retorna apenas os trabalhos de backup que correspondem ao recurso especificado Nome de recurso da Amazon (ARN).

[ByResourceType](#) (p. 284)

Retorna somente trabalhos de backup para os recursos especificados:

- `DynamoDB` para o Amazon DynamoDB
- `EBS` para o Amazon Elastic Block Store
- `EC2` para o Amazon Elastic Compute Cloud
- `EFS` para o Amazon Elastic File System
- `RDS` para o Amazon Relational Database Service
- `Aurora` para Amazon Aurora
- `Storage Gateway` para AWS Storage Gateway

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

BYState (p. 284)

Retorna apenas trabalhos de backup que estão no estado especificado.

Valores válidos: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED

MaxResults (p. 284)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

NextToken (p. 284)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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",
      "PercentDone": "string",
      "RecoveryPointArn": "string",
      "ResourceArn": "string",
      "ResourceType": "string",
      "StartBy": number,
      "State": "string",
      "StatusMessage": "string"
    },
    {
      "NextToken": "string"
    }
  ]
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupJobs](#) (p. 285)

Uma matriz de estruturas contendo metadados sobre seus trabalhos de backup retornados no formato JSON.

Type: Array[BackupJob](#) (p. 354)objects

[NextToken](#) (p. 285)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupPlans

Retorna uma lista de todos os planos de backup ativos para uma conta autenticada. A lista contém informações como Amazon Resource Names (ARNs), IDs de plano, datas de criação e exclusão, IDs de versão, nomes de planos e IDs de solicitação de criador.

Sintaxe da solicitação

```
GET /backup/plans/?includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken
HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[IncluídoExcluído](#) (p. 287)

Um valor booleano com um valor padrão de `FALSE` que retorna planos de backup excluídos quando definido como `TRUE`.

[MaxResults](#) (p. 287)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

[NextToken](#) (p. 287)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupPlansList \(p. 287\)](#)

Uma matriz de itens de lista de planos de backup contendo metadados sobre seus planos de backup salvos.

Type: Array [BackupPlansListMember \(p. 360\)](#) objects

[NextToken \(p. 287\)](#)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupPlanTemplates

Retorna metadados dos modelos de plano de backup salvos, incluindo o ID do modelo, o nome e as datas de criação e exclusão.

Sintaxe da solicitação

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[MaxResults](#) (p. 290)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

[NextToken](#) (p. 290)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupPlanTemplatesList](#) (p. 290)

Uma matriz de itens de lista de modelos contendo metadados sobre seus modelos salvos.

Type: Array [BackupPlanTemplatesListMember](#) (p. 362) objects

[NextToken \(p. 290\)](#)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupPlanVersions

Retorna metadados de versão de seus planos de backup, incluindo Amazon Resource Names (ARNs), IDs de plano 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

A solicitação usa os seguintes parâmetros de URI.

[BackupPlanId](#) (p. 292)

Identifica exclusivamente um plano de backup.

: obrigatório Sim

[MaxResults](#) (p. 292)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

[NextToken](#) (p. 292)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupPlanVersionsList](#) (p. 292)

Uma matriz de itens de lista de versões contendo metadados sobre seus planos de backup.

Type: Array[BackupPlansListMember](#) (p. 360)objects

[NextToken](#) (p. 292)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)

- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupSelections

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

A solicitação usa os seguintes parâmetros de URI.

[BackupPlanId](#) (p. 295)

Identifica exclusivamente um plano de backup.

: obrigatório Sim

[MaxResults](#) (p. 295)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

[NextToken](#) (p. 295)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupSelectionsList \(p. 295\)](#)

Uma matriz de itens de lista de seleção de backup contendo metadados sobre cada recurso na lista.

Type: Array[BackupSelectionsListMember \(p. 368\)](#)objects

[NextToken \(p. 295\)](#)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListBackupVaults

Retorna uma lista de contêineres de armazenamento de ponto de recuperação juntamente com informações sobre eles.

Sintaxe da solicitação

```
GET /backup-vaults/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

MaxResults (p. 298)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

NextToken (p. 298)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar *maxResults* Número de itens, *NextToken* permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultList": [
    {
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CreationDate": number,
      "CreatorRequestId": "string",
      "EncryptionKeyArn": "string",
      "NumberOfRecoveryPoints": number
    }
  ],
  "NextToken": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

BackupVaultList (p. 298)

Uma matriz de membros da lista do cofre de backup contendo metadados do cofre, incluindo Nome de recurso da Amazon (ARN), nome de exibição, data de criação, número de pontos de

recuperação salvos e informações de criptografia se os recursos salvos no cofre de backup estiverem criptografados.

Type: Array [BackupVaultListMember](#) (p. 370) objects

[NextToken](#) (p. 298)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListCopyJobs

Retorna metadados sobre seus trabalhos de cópia.

Sintaxe da solicitação

```
GET /copy-jobs/?
accountId=ByAccountId&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&destinationVaultArn=ByDestinationVaultArn&resourceArn=ByResourceArn&resourceType=ByResourceType&state=ByState
HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[PorAccountId](#) (p. 300)

O ID da conta a partir do qual listar os trabalhos. Retorna apenas trabalhos de cópia associados ao ID de conta especificado.

Padrão: `^[0-9]{12}$`

[byCreateDafter](#) (p. 300)

Retorna apenas trabalhos de cópia que foram criados após a data especificada.

[PorCreatedBefore](#) (p. 300)

Retorna apenas trabalhos de cópia que foram criados antes da data especificada.

[byDestinationVaultARN](#) (p. 300)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup de origem para copiar, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

[ByResourceArn](#) (p. 300)

Retorna apenas os trabalhos de cópia que correspondem ao recurso especificado Nome de recurso da Amazon (ARN).

[ByResourceType](#) (p. 300)

Retorna somente trabalhos de backup para os recursos especificados:

- `DynamoDB` para o Amazon DynamoDB
- `EBSAmazon` Elastic Block Store
- `EC2` para o Amazon Elastic Compute Cloud
- `EFS` para o Amazon Elastic File System
- `RDS` para o Amazon Relational Database Service
- `Aurora` para Amazon Aurora
- `Storage Gateway` para AWS Storage Gateway

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

[BYState](#) (p. 300)

Retorna apenas trabalhos de cópia que estão no estado especificado.

Valores válidos: `CREATED` | `RUNNING` | `COMPLETED` | `FAILED`

MaxResults (p. 300)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

NextToken (p. 300)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar MaxResults número de itens, NextToken permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "CopyJobs": [
    {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "CompletionDate": number,
      "CopyJobId": "string",
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
      },
      "CreationDate": number,
      "DestinationBackupVaultArn": "string",
      "DestinationRecoveryPointArn": "string",
      "IamRoleArn": "string",
      "ResourceArn": "string",
      "ResourceType": "string",
      "SourceBackupVaultArn": "string",
      "SourceRecoveryPointArn": "string",
      "State": "string",
      "StatusMessage": "string"
    }
  ],
  "NextToken": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

CopyJobs (p. 301)

Uma matriz de estruturas contendo metadados sobre seus trabalhos de cópia retornados no formato JSON.

Type: ArrayCopyJob (p. 375)objects

[NextToken \(p. 301\)](#)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar MaxResults número de itens, NextToken permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListProtectedResources

Retorna uma matriz de recursos do backup com sucesso pelo AWS Backup, incluindo a hora em que o recurso foi salvo, um nome de recurso da Amazon (ARN) do recurso e um tipo de recurso.

Sintaxe da solicitação

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

MaxResults (p. 303)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

NextToken (p. 303)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Results": [
    {
      "LastBackupTime": number,
      "ResourceArn": "string",
      "ResourceType": "string"
    }
  ]
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

NextToken (p. 303)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

[Resultados \(p. 303\)](#)

Um conjunto de recursos com backup bem-sucedido do AWS Backup incluindo a hora em que o recurso foi salvo, um nome de recurso da Amazon (ARN) do recurso e um tipo de recurso.

Type: Array [ProtectedResource \(p. 379\)](#) objects

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListRecoveryPointsByBackupVault

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&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&maxResults=MaxRes  
HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 305)

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 oAWSRegião onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

[byBackupPlanId](#) (p. 305)

Retorna apenas pontos de recuperação que correspondem ao ID do plano de backup especificado.

[byCreateDafter](#) (p. 305)

Retorna apenas pontos de recuperação que foram criados após o carimbo de data/hora especificado.

[PorCreatedBefore](#) (p. 305)

Retorna apenas pontos de recuperação que foram criados antes do carimbo de data/hora especificado.

[ByResourceArn](#) (p. 305)

Retorna apenas pontos de recuperação que correspondem ao recurso especificado do nome de recurso da Amazon (ARN).

[ByResourceType](#) (p. 305)

Retorna apenas pontos de recuperação que correspondem ao tipo de recurso especificado.

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

[MaxResults](#) (p. 305)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

[NextToken](#) (p. 305)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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,
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
      },
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "IamRoleArn": "string",
      "IsEncrypted": boolean,
      "LastRestoreTime": number,
      "Lifecycle": {
        "DeleteAfterDays": number,
        "MoveToColdStorageAfterDays": number
      },
      "RecoveryPointArn": "string",
      "ResourceArn": "string",
      "ResourceType": "string",
      "SourceBackupVaultArn": "string",
      "Status": "string"
    }
  ]
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[NextToken](#) (p. 306)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

[Pontos de recuperação](#) (p. 306)

Uma matriz de objetos que contém informações detalhadas sobre pontos de recuperação salvos em um cofre de backup.

Type: Array [RecoveryPointByBackupVault](#) (p. 380) objects

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListRecoveryPointsByResource

Retorna informações detalhadas sobre todos os pontos de recuperação do tipo especificado por um recurso Amazon Resource Name (ARN).

Note

Para EFS e EC2, essa ação lista apenas os pontos de recuperação criados pelo AWS Backup.

Sintaxe da solicitação

```
GET /resources/resourceArn/recovery-points/?maxResults=MaxResults&nextToken=NextToken
HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

MaxResults (p. 308)

O número máximo de itens a serem retornados.

Note

O Amazon RDS requer um valor de pelo menos 20.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

NextToken (p. 308)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

resourceArn (p. 308)

Um ARN que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RecoveryPoints": [
    {
      "BackupSizeBytes": number,
      "BackupVaultName": "string",
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "RecoveryPointArn": "string",
      "Status": "string"
    }
  ]
}
```

```
}  
  ]  
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[NextToken](#) (p. 308)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

[Pontos de recuperação](#) (p. 308)

Uma matriz de objetos que contém informações detalhadas sobre pontos de recuperação do tipo de recurso especificado.

Note

Somente os pontos de recuperação EFS e EC2 retornam `BackupVaultName`.

Type: Array [RecoveryPointByResource](#) (p. 383) objects

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListRestoreJobs

Retorna uma lista de trabalhos que AWS Backup iniciou para restaurar um recurso salvo, incluindo metadados sobre o processo de recuperação.

Sintaxe da solicitação

```
GET /restore-jobs/?
accountId=ByAccountId&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&maxResults=MaxResults&
HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[PorAccountId](#) (p. 311)

O ID da conta a partir do qual listar os trabalhos. Retorna apenas trabalhos de restauração associados ao ID de conta especificado.

Padrão: `^[0-9]{12}$`

[byCreateDafter](#) (p. 311)

Retorna somente trabalhos de restauração que foram criados após a data especificada.

[PorCreatedBefore](#) (p. 311)

Retorna somente trabalhos de restauração que foram criados antes da data especificada.

[BYStatus](#) (p. 311)

Retorna apenas os trabalhos de restauração associados ao status do trabalho especificado.

Valores válidos: `PENDING` | `RUNNING` | `COMPLETED` | `ABORTED` | `FAILED`

[MaxResults](#) (p. 311)

O número máximo de itens a serem retornados.

Intervalo válido Valor mínimo de 1. Valor máximo de 1000.

[NextToken](#) (p. 311)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
```

```
"RestoreJobs": [
  {
    "AccountId": "string",
    "BackupSizeInBytes": number,
    "CompletionDate": number,
    "CreatedResourceArn": "string",
    "CreationDate": number,
    "ExpectedCompletionTimeMinutes": number,
    "IamRoleArn": "string",
    "PercentDone": "string",
    "RecoveryPointArn": "string",
    "ResourceType": "string",
    "RestoreJobId": "string",
    "Status": "string",
    "StatusMessage": "string"
  }
]
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[NextToken \(p. 311\)](#)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

[RestoreJobs \(p. 311\)](#)

Uma matriz de objetos que contêm informações detalhadas sobre trabalhos para restaurar recursos salvos.

Type: Array [RestoreJobsListMember \(p. 386\)](#) objects

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListTags

Retorna uma lista de pares chave-valor atribuídos a um ponto de recuperação de destino, plano de backup ou cofre de backup.

Note

`ListTags` atualmente só são compatíveis com backups do Amazon EFS.

Sintaxe da solicitação

```
GET /tags/resourceArn?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

`MaxResults` (p. 314)

O número máximo de itens a serem retornados.

Intervalo válido: Valor mínimo de 1. Valor máximo de 1000.

`NextToken` (p. 314)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

`resourceArn` (p. 314)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um recurso. O formato do ARN depende do tipo de recurso. Alvos válidos para `ListTags` são pontos de recuperação, planos de backup e cofres de backup.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[NextToken \(p. 314\)](#)

O próximo item após uma lista parcial de itens devolvidos. Por exemplo, se uma solicitação for feita para retornar `maxResults` Número de itens, `NextToken` permite que você retorne mais itens em sua lista começando no local apontado pelo próximo token.

Type: String

[Tags \(p. 314\)](#)

Para ajudar a organizar seus recursos, você pode atribuir seus próprios metadados aos recursos que criar. Cada tag é um par de chave-valor.

Type: Mapa de string para string

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

PutBackupVaultAccessPolicy

Define uma política com base em recursos 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

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 317)

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 oAWSRegião onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[Política](#) (p. 317)

O documento da política de acesso ao cofre de backup no formato JSON.

Type: String

: obrigatório Não

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

PutBackupVaultNotifications

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

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 319)

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 oAWSRegião onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[BackupVaultEvents](#) (p. 319)

Uma matriz de eventos que indicam o status de trabalhos para recursos de backup para o cofre de backup.

Note

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 e RECOVERY_POINT_MODIFIED.
Para localizar trabalhos de backup com falha, useBACKUP_JOB_COMPLETEDe filtre usando metadados de evento.
Outros eventos na lista a seguir estão obsoletos.

Type: 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

: obrigatório Sim

[SNSTopicArn \(p. 319\)](#)

o nome de recurso da Amazon (ARN) que especifica o tópico para eventos de um cofre de backup, por exemplo, `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Type: String

: obrigatório Sim

Sintaxe da resposta

`HTTP/1.1 200`

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)

- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

StartBackupJob

Inicia um job 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
  },
  "RecoveryPointTags": {
    "string" : "string"
  },
  "ResourceArn": "string",
  "StartWindowMinutes": number
}
```

Parâmetros da solicitação

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[BackupOptions \(p. 322\)](#)

Especifica a opção de backup para um recurso selecionado. Essa opção só está disponível para trabalhos de backup do Windows VSS.

Valores válidos: Defina para "WindowsVSS": "enabled" para habilitar a opção de backup do WindowsVSS e criar um backup do Windows VSS. Defina como "WindowsVSS": "desabilitado" para criar um backup regular. A opção WindowSVSS não é habilitada por padrão.

Type: Mapa de string para string

Pattern: `^[a-zA-Z0-9\-_\.\]{1,50}$`

Pattern: `^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Não

[BackupVaultName \(p. 322\)](#)

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 oAWSRegião onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

[CompleteWindowMinutes \(p. 322\)](#)

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. Ele não adiciona tempo adicional para `StartWindowMinutes` se o backup foi iniciado mais tarde do que o agendado.

Type: Long

: obrigatório Não

[IamRoleArn \(p. 322\)](#)

Especifica o ARN da função do IAM usado para criar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

: obrigatório Sim

[IdempotencyToken \(p. 322\)](#)

Uma string escolhida pelo cliente que pode ser usada para distinguir entre chamadas idênticas para `StartBackupJob`. Repetir uma solicitação bem-sucedida com o mesmo token de idempotency resultará em uma mensagem de `success` sem nenhuma ação tomada.

Type: String

: obrigatório Não

[Ciclo de vida \(p. 322\)](#)

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento "frio" e quando ele expira. O AWS Backup fará a transferência e a expiração de 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 "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio".

Tipo: objeto [Lifecycle \(p. 378\)](#)

: obrigatório Não

[RecoveryPointTags \(p. 322\)](#)

Para ajudar a organizar seus recursos, você pode atribuir seus próprios metadados aos recursos que criar. Cada tag é um par de chave-valor.

Type: Mapa de string para string

: obrigatório Não

[ResourceArn \(p. 322\)](#)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um recurso. O formato do ARN depende do tipo de recurso.

Type: String

: obrigatório Sim

[StartWindowMinutes \(p. 322\)](#)

Um valor em minutos após um backup ser programado para que um trabalho seja cancelado, se ele não for iniciado com êxito. Esse valor é opcional e o padrão é 8 horas.

Type: Long

: obrigatório Não

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupJobId": "string",
  "CreationDate": number,
  "RecoveryPointArn": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupJobID \(p. 324\)](#)

Identificar exclusivamente uma solicitação para AWS Backup para fazer backup de um recurso.

Type: String

[CreationDate \(p. 324\)](#)

A data e hora em que um trabalho de backup é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[RecoveryPointArn \(p. 324\)](#)

Um ARN que identifica exclusivamente um ponto de recuperação; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`InvalidRequestException`

indica que algo está 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, um número máximo de itens permitidos em uma solicitação.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

StartCopyJob

Inicia um trabalho para criar uma cópia única do recurso especificado.

Não oferece suporte a 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
  },
  "RecoveryPointArn": "string",
  "SourceBackupVaultName": "string"
}
```

Parâmetros da solicitação

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[DestinationBackupVaultArn](#) (p. 326)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup de destino para copiar, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

: obrigatório Sim

[IamRoleArn](#) (p. 326)

Especifica o ARN da função do IAM usado para copiar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

: obrigatório Sim

[IdempotencyToken](#) (p. 326)

Uma string escolhida pelo cliente que pode ser usada para distinguir entre chamadas idênticas para `StartCopyJob`. Repetir uma solicitação bem-sucedida com o mesmo token de idempotency resultará em uma mensagem de sucesso sem nenhuma ação tomada.

Type: String

: obrigatório Não

Ciclo de vida (p. 326)

Contém uma matriz de `TransitionOs` objetos que especificam o tempo, em dias, para que um ponto de recuperação seja alterado para armazenamento de baixa atividade ou seja excluído.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, no console, a configuração de "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS do podem ser transferidos para armazenamento "frio".

Tipo: objeto [Lifecycle](#) (p. 378)

: obrigatório Não

[RecoveryPointArn](#) (p. 326)

Um ARN que identifica exclusivamente um ponto de recuperação a ser usado para o trabalho de cópia; por exemplo, `arn:aws:backup:us-east-1:123456789012:Ponto de recuperação:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

: obrigatório Sim

[sourceBackupVaultName](#) (p. 326)

O nome de um contêiner de origem lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e o `AWSRegião` onde foram criadas. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
  "CopyJobId": "string",
  "CreationDate": number
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[CopyJobID](#) (p. 327)

Identificar exclusivamente um trabalho de cópia.

Type: String

[CreationDate \(p. 327\)](#)

A data e hora em que um trabalho de cópia é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`InvalidRequestException`

indica que algo está 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, um número máximo de itens permitidos em uma solicitação.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)

- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

StartRestoreJob

Recupera o recurso salvo identificado por um Nome de recurso da Amazon (ARN).

Sintaxe da solicitação

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "Metadata": {
    "string" : "string"
  },
  "RecoveryPointArn": "string",
  "ResourceType": "string"
}
```

Parâmetros da solicitação

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[IamRoleArn \(p. 330\)](#)

O nome de recurso da Amazon (ARN) da função do IAM que AWS Backup usa para criar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

: obrigatório Sim

[IdempotencyToken \(p. 330\)](#)

Uma string escolhida pelo cliente que pode ser usada para distinguir entre chamadas idênticas para `StartRestoreJob`. Repetir uma solicitação bem-sucedida com o mesmo token de idempotency resultará em uma mensagem de sucesso sem nenhuma ação tomada.

Type: String

: obrigatório Não

[Metadados \(p. 330\)](#)

Um conjunto de pares de chave/valor de metadados. Contém informações, como um nome de recurso, necessárias para restaurar um ponto de recuperação.

Você pode obter metadados de configuração sobre um recurso no momento em que foi feito o backup chamando `GetRecoveryPointRestoreMetadata`. No entanto, valores além daqueles fornecidos pelo `GetRecoveryPointRestoreMetadata` talvez seja necessário restaurar um recurso. Por exemplo, pode ser necessário fornecer um novo nome de recurso, se o original já existir.

Você precisa especificar metadados específicos para restaurar uma instância do Amazon Elastic File System (Amazon EFS):

- `file-system-id`: a ID do sistema de arquivos do Amazon EFS do que é submetido a backup pelo AWS Backup. Restaurado em `GetRecoveryPointRestoreMetadata`.
- `Encrypted`: um valor booleano que, quando verdadeiro, especifica que o sistema de arquivos é criptografado. Se `KmsKeyId` for especificado, `Encrypted` deverá ser definido como `true`.
- `KmsKeyId`: Especifica o AWS Chave KMS usada para criptografar o sistema de arquivos restaurado. Você pode especificar uma chave de outro AWS desde que a chave seja devidamente compartilhada com a sua conta através do AWS KMS.
- `PerformanceMode`: indica o modo de taxa de transferência do sistema de arquivos.
- `CreationToken`: um valor fornecido pelo usuário que garante a exclusividade (idempotência) da solicitação.
- `newFileSystem`: Um valor booleano que, se verdadeiro, especifica que o ponto de recuperação foi restaurado para um novo sistema de arquivos do Amazon EFS.
- `ItemsToRestore` : Uma matriz de uma a cinco strings em que cada string é um caminho de arquivo. Usar `ItemsToRestorePara` restaurar arquivos ou diretórios específicos em vez de todo o sistema de arquivos. Esse parâmetro é opcional. Por exemplo, `"itemsToRestore":["\"/my.test\"]`.

Type: Mapa de string para string

: obrigatório Sim

[RecoveryPointArn \(p. 330\)](#)

Um ARN que identifica exclusivamente um ponto de recuperação; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

: obrigatório Sim

[ResourceType \(p. 330\)](#)

Inicia um trabalho para restaurar um ponto de recuperação para um dos seguintes recursos:

- `DynamoDB` para o Amazon DynamoDB
- `EBSAmazon` Elastic Block Store
- `EC2` para o Amazon Elastic Compute Cloud
- `EFS` para o Amazon Elastic File System
- `RDS` para o Amazon Relational Database Service
- `Aurora` para Amazon Aurora
- `Storage Gateway` para AWS Storage Gateway

Type: 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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[RestoreJobid](#) (p. 331)

Identifica exclusivamente o trabalho que restaura um ponto de recuperação.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

StopBackupJob

Tenta cancelar um trabalho para criar um backup único de um recurso.

Sintaxe da solicitação

```
POST /backup-jobs/backupJobId HTTP/1.1
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupJobID](#) (p. 333)

Identificar exclusivamente uma solicitação para AWS Backup para fazer backup de um recurso.

: obrigatório Sim

Corpo da solicitação

A solicitação não tem um corpo de solicitação.

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

InvalidRequestException

indica que algo está errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

TagResource

Atribui um conjunto de pares de chave-valor a um ponto de recuperação, plano de backup ou cofre de backup identificado por um Nome de recurso da Amazon (ARN).

Sintaxe da solicitação

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
  "Tags": {
    "string" : "string"
  }
}
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[resourceArn](#) (p. 335)

Um ARN que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso marcado.

: obrigatório Sim

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[Tags](#) (p. 335)

Pares de chave-valor que são usados para ajudar a organizar seus recursos. Você pode atribuir seus próprios metadados aos recursos que criar.

Type: Mapa de string para string

: obrigatório Sim

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

InvalidParameterValueException

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

LimitExceededException

Um limite na solicitação foi excedido; por exemplo, um número máximo de itens permitidos em uma solicitação.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UntagResource

Remove um conjunto de pares de chave-valor de um ponto de recuperação, plano de backup ou cofre de backup identificado por um Amazon Resource Name (ARN)

Sintaxe da solicitação

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
  "TagKeyList": [ "string" ]
}
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[resourceArn](#) (p. 337)

Um ARN que identifica de forma exclusiva um recurso. O formato do ARN depende do tipo de recurso marcado.

: obrigatório Sim

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[TagKeyList](#) (p. 337)

Uma lista de chaves para identificar quais tags chave-valor devem ser removidas de um recurso.

Type: Matriz de strings

: obrigatório Sim

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ResourceNotFoundException

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateBackupPlan

Atualiza um plano de backup existente identificado pelo `seubackupPlanId` com o documento de entrada no formato JSON. A nova versão é identificada exclusivamente por `umVersionId`.

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
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "Lifecycle": {
          "DeleteAfterDays": number,
          "MoveToColdStorageAfterDays": number
        },
        "RecoveryPointTags": {
          "string": "string"
        },
        "RuleName": "string",
        "ScheduleExpression": "string",
        "StartWindowMinutes": number,
        "TargetBackupVaultName": "string"
      }
    ]
  }
}
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupPlanId](#) (p. 339)

Identifica exclusivamente um plano de backup.

: obrigatório Sim

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[BackupPlan](#) (p. 339)

Especifica o corpo de um plano de backup. Inclui um `BackupPlanName` e um ou mais conjuntos de `Rules`.

Tipo: objeto [BackupPlanInput](#) (p. 359)

: obrigatório 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 reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[AdvancedBackupSettings](#) (p. 340)

Contém uma lista de `BackupOptions` para cada tipo de recurso.

Type: Array [AdvancedBackupSetting](#) (p. 352) objects

[BackupPlanArn](#) (p. 340)

Um nome de 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`.

Type: String

[BackupPlanId](#) (p. 340)

Identifica exclusivamente um plano de backup.

Type: String

[CreationDate \(p. 340\)](#)

A data e hora em que um plano de backup é atualizado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

[VersionId \(p. 340\)](#)

Strings Unicode exclusivas geradas aleatoriamente, codificadas em UTF-8 que têm no máximo 1.024 bytes. IDs de versão não podem ser editados.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns \(p. 388\)](#).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateGlobalSettings

Atualiza se o AWS tem optado por fazer backup entre contas. Retorna um erro se a conta não for uma conta de gerenciamento de Organizations. Usar `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

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[globalSettings](#) (p. 343)

Um valor para `isCrossAccountBackupEnabled` de uma região. Exemplo: `update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

Type: Mapa de string para string

: obrigatório Não

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

InvalidRequestException

indica que algo está errado com a entrada da solicitação. Por exemplo, um parâmetro é do tipo errado.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateRecoveryPointLifecycle

Define o ciclo de vida de transição de um ponto de recuperação.

O ciclo de vida define quando um recurso protegido é passado para armazenamento de baixa atividade e quando expira. AWS Backup faz com que os backups sejam transferidos e expirados 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 "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio".

Não oferece suporte a backups contínuos.

Sintaxe da solicitação

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
  "Lifecycle": {
    "DeleteAfterDays": number,
    "MoveToColdStorageAfterDays": number
  }
}
```

Parâmetros da solicitação

A solicitação usa os seguintes parâmetros de URI.

[BackupVaultName](#) (p. 345)

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 o AWS Região onde foram criadas. Eles consistem em letras minúsculas, números e hífens.

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

[RecoveryPointArn](#) (p. 345)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente 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.

Ciclo de vida (p. 345)

O ciclo de vida define quando um recurso protegido é passado para armazenamento de baixa atividade e quando expira. AWS Backup faz com que os backups sejam transferidos e expirados 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 "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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](#) (p. 378)

: 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
  },
  "RecoveryPointArn": "string"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta HTTP 200.

Os seguintes dados são retornados no formato JSON pelo serviço.

[BackupVaultArn](#) (p. 346)

Um ARN que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

[Ciclo de vida calculado](#) (p. 346)

A `CalculatedLifecycle` objeto contendo `DeleteAt` e `MoveToColdStorageAt` timestamps.

Tipo: objeto [CalculatedLifecycle](#) (p. 372)

[Ciclo de vida](#) (p. 346)

O ciclo de vida define quando um recurso protegido é passado para armazenamento de baixa atividade e quando expira. AWS Backup faz com que os backups sejam transferidos e expirados 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 "número de dias para a expiração" deve ser 90 dias maior do que

a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS do podem ser transferidos para armazenamento "frio".

Tipo: objeto [Lifecycle](#) (p. 378)

[RecoveryPointArn](#) (p. 346)

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um ponto de recuperação, por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

`MissingParameterValueException`

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

`ResourceNotFoundException`

Um recurso que é necessário para a ação não existe.

Código de status HTTP: 400

`ServiceUnavailableException`

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

UpdateRegionSettings

Atualiza as configurações atuais de opção pelo serviço para a Região. Se o service-opt-in estiver habilitado para um serviço, AWS Backup tenta proteger os recursos desse serviço nesta região, quando o recurso está incluído em um backup sob demanda ou plano de backup agendado. Caso contrário, AWS Backup não tenta proteger os recursos desse serviço nesta Região. Usar `DescribeRegionSettings` para determinar os tipos de recursos suportados.

Sintaxe da solicitação

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
  "ResourceTypeOptInPreference": {
    "string" : boolean
  }
}
```

Parâmetros da solicitação

A solicitação não usa parâmetros de URI.

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

[ResourceTypeOptInPreference](#) (p. 349)

Atualiza a lista de serviços juntamente com as preferências de aceitação para a Região.

Type: Mapa de string para booleano

Pattern: `^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Não

Sintaxe da resposta

```
HTTP/1.1 200
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Errors

Para obter informações sobre os erros que são comuns a todas as ações, consulte [Erros comuns](#) (p. 388).

`InvalidParameterValueException`

indica que algo está errado com o valor de um parâmetro. Por exemplo, o valor está fora de intervalo.

Código de status HTTP: 400

MissingParameterValueException

Indica que um parâmetro obrigatório está ausente.

Código de status HTTP: 400

ServiceUnavailableException

A solicitação falhou 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 de linguagem, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

Tipos de dados

Os seguintes tipos de dados são compatíveis:

- [AdvancedBackupSetting](#) (p. 352)
- [BackupJob](#) (p. 354)
- [BackupPlan](#) (p. 358)
- [BackupPlanInput](#) (p. 359)
- [BackupPlansListMember](#) (p. 360)
- [BackupPlanTemplatesListMember](#) (p. 362)
- [BackupRule](#) (p. 363)
- [BackupRuleInput](#) (p. 365)
- [BackupSelection](#) (p. 367)
- [BackupSelectionsListMember](#) (p. 368)
- [BackupVaultListMember](#) (p. 370)
- [CalculatedLifecycle](#) (p. 372)
- [Condition](#) (p. 373)
- [CopyAction](#) (p. 374)
- [CopyJob](#) (p. 375)
- [Lifecycle](#) (p. 378)
- [ProtectedResource](#) (p. 379)
- [RecoveryPointByBackupVault](#) (p. 380)

- [RecoveryPointByResource](#) (p. 383)
- [RecoveryPointCreator](#) (p. 385)
- [RestoreJobsListMember](#) (p. 386)

AdvancedBackupSetting

Uma lista de opções de backup para cada tipo de recurso.

Contents

BackupOptions

Especifica a opção de backup para um recurso selecionado. Essa opção só está disponível para trabalhos de backup do Windows VSS.

Valores válidos:

Defina para "windowsVSS": "enabled" para habilitar a opção de backup do WindowsVSS e criar um backup do Windows VSS.

Defina para "windowsVSS": "disabled" para criar um backup regular. A opção WindowsVSS não está habilitada por padrão.

Se você especificar uma opção inválida, você obtém um `InvalidParameterValueException` exceção.

Para obter mais informações sobre backups do Windows VSS, consulte [Criando um Backup do Windows habilitado para VSS](#).

Type: Mapa de string para string

Pattern de chave `^[a-zA-Z0-9\-_\.\]{1,50}$`

Valor Pattern: `^[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 com suporte são as instâncias do Amazon EC2 com Windows VSS. Para obter um exemplo do CloudFormation, consulte o [modelo de exemplo do CloudFormation para habilitar o Windows VSS](#) no AWS Backup Guia do usuário do.

Valores válidos: EC2.

Type: 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 de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupJob

Contém informações detalhadas sobre um trabalho de backup.

Contents

AccountId

O ID da conta da à qual pertence o trabalho de backup.

Type: String

Padrão: `^[0-9]{12}$`

: obrigatório Não

BackupJobID

Identificar exclusivamente uma solicitação paraAWS Backuppara fazer backup de um recurso.

Type: String

: obrigatório Não

BackupOptions

Especifica a opção de backup para um recurso selecionado. Essa opção só está disponível para trabalhos de backup do Windows VSS.

Valores válidos: Defina para"windowsvss": "enabled"para habilitar a opção de backup do WindowsVSS e criar um backup do Windows VSS. Defina como "WindowsVSS": "desabilitado" para criar um backup regular. Se você especificar uma opção inválida, você obtém umInvalidParameterValueExceptionExceção.

Type: Mapa de string para string

Pattern de chave`^[a-zA-Z0-9\-_\.\]{1,50}$`

Valor Pattern:`^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Não

BackupSizeInBytes

O tamanho, em bytes, de um backup.

Type: Long

: obrigatório Não

BackupType

Representa o tipo de backup para um trabalho de backup.

Type: String

: obrigatório Não

BackupVaultArn

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo,`arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

: 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 para a conta usada para criá-los e oAWSRegião da em que são criadas. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Não

BytesTransferred

O tamanho em bytes transferidos para um cofre de backup no momento em que o status do trabalho foi consultado.

Type: Long

: obrigatório Não

CompletionDate

A data e hora em que um trabalho para criar um trabalho de backup é concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor deCompletionDateé preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

CreatedBy

Contém informações de identificação sobre a criação de um trabalho de backup, incluindo oBackupPlanArn,BackupPlanId,BackupPlanVersion, eBackupRuleIddo plano de backup usado para criá-lo.

Tipo: objeto [RecoveryPointCreator](#) (p. 385)

: obrigatório Não

CreationDate

A data e hora em que um trabalho de backup é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor deCreationDateé preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

ExpectedCompletionDate

A data e hora em que um trabalho para fazer backup dos recursos é esperado para ser concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor deExpectedCompletionDateé preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

IamRoleArn

Especifica o ARN da função do IAM usado para criar o ponto de recuperação de destino. As funções do IAM que não sejam a função padrão devem incluir `AWSBackup` ou `AwsBackup` no nome da função. Por exemplo, `arn:aws:iam::123456789012:role/AWSBackupRDSAccess`. Nomes de função sem essas cadeias de caracteres não têm permissões para executar trabalhos de backup.

Type: String

: obrigatório Não

Percentdone

Contém uma porcentagem estimada de conclusão de um trabalho no momento em que o status do job foi consultado.

Type: String

: obrigatório Não

RecoveryPointArn

Um ARN que identifica exclusivamente um ponto de recuperação; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

: obrigatório Não

ResourceArn

Um ARN que identifica exclusivamente um recurso. O formato do ARN depende do tipo de recurso.

Type: String

: obrigatório Não

ResourceType

O tipo de AWSO recurso será feito em backup; 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 VSS Windows, o único tipo de recurso com suporte é o Amazon EC2.

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Não

StartBy

Especifica o tempo no formato Unix e Tempo Universal Coordenado (UTC) em que um trabalho de backup deve ser iniciado para que ele seja cancelado. O valor é calculado adicionando a janela inicial à hora programada. Portanto, se o horário agendado fosse 18:00 PM e a janela de início for de 2 horas, o `StartBy` seria 20h na data especificada. O valor de `StartBy` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

Estado

O estado atual de um ponto de recuperação de recursos.

Type: String

Valores válidos: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED

: obrigatório Não

StatusMessage

Uma mensagem detalhada explicando o status do trabalho para fazer backup de um recurso.

Type: String

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupPlan

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 AWS recursos da AWS.

Contents

AdvancedBackupSettings

Contém uma lista de `BackupOptions` Para cada tipo de recurso.

Type: Array [AdvancedBackupSetting \(p. 352\)](#) objects

: obrigatório Não

BackupPlanName

O nome de exibição de um plano de backup.

Type: String

: obrigatório Sim

Regras

Uma matriz de objetos `BackupRule`, em que cada um especifica uma tarefa programada que é usada para fazer backup de uma seleção de recursos.

Type: Array [BackupRule \(p. 363\)](#) objects

: obrigatório Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupPlanInput

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 AWS recursos da AWS.

Contents

AdvancedBackupSettings

Especifica uma lista de `BackupOptions` Para cada tipo de recurso. Estas definições só estão disponíveis para trabalhos de cópia de segurança do Windows VSS.

Type: Array [AdvancedBackupSetting](#) (p. 352) objects

: obrigatório Não

BackupPlanName

O nome de exibição opcional de um plano de backup.

Type: String

: obrigatório Sim

Regras

Uma matriz de objetos `BackupRule`, em que cada um especifica uma tarefa programada que é usada para fazer backup de uma seleção de recursos.

Type: Array [BackupRuleInput](#) (p. 365) objects

: obrigatório Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupPlansListMember

Contém metadados sobre um plano de backup.

Contents

AdvancedBackupSettings

Contém uma lista de `BackupOptions` para um tipo de recurso.

Type: Array [AdvancedBackupSetting](#) (p. 352) objects

: obrigatório Não

BackupPlanArn

Um nome de 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`.

Type: String

: obrigatório Não

BackupPlanId

Identifica exclusivamente um plano de backup.

Type: String

: obrigatório Não

BackupPlanName

O nome de exibição de um plano de backup salvo.

Type: String

: obrigatório Não

CreationDate

A data e hora em que um plano de backup de recurso é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor `1516925490.087` representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

CreatorRequestId

Uma string exclusiva que identifica a solicitação e permite que solicitações com falha sejam repetidas sem o risco de executar a operação duas vezes.

Type: String

: obrigatório Não

DeletionDate

A data e hora em que um plano de backup é excluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `DeletionDate` é preciso para milissegundos. Por exemplo, o valor `1516925490.087` representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

LastExecutionDate

A última vez que um trabalho para fazer backup de recursos foi executado com essa regra. Uma data e hora, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastExecutionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: 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.

Type: String

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupPlanTemplatesListMember

Um objeto que especifica metadados associados a um modelo de plano de backup.

Contents

BackupPlantemplateID

Identifica exclusivamente um modelo de plano de backup armazenado.

Type: String

: obrigatório Não

BackupPlantemplateName

O nome de exibição opcional de um modelo de plano de backup.

Type: String

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupRule

Especifica uma tarefa programada usada para fazer backup de uma seleção de recursos.

Contents

CompletionWindowMinutes

Um valor em minutos após um trabalho de backup ser iniciado com êxito para que ele seja concluído ou cancelado pelo AWS Backup. Este valor é opcional.

Type: Long

: obrigatório Não

CopyActions

Uma matriz de `CopyAction` objetos, que contém os detalhes da operação de cópia.

Type: Array [CopyAction](#) (p. 374) objects

: obrigatório Não

EnableContinuousBackup

Especifica se o AWS Backup cria backups contínuos. Verdadeiro causa o AWS Backup a criar backups contínuos capazes de PITR (point-in-time restore - restauração point-in-time). Causas falsas (ou não especificadas) o AWS Backup a criar backups de snapshot.

Type: Booleano

: obrigatório Não

Ciclo de vida

O ciclo de vida define quando um recurso protegido é passado para armazenamento de baixa atividade e quando expira. O AWS Backup faz com que os backups sejam transferidos e expirados 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 "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio".

Tipo: objeto [Lifecycle](#) (p. 378)

: obrigatório Não

RecoveryPointTags

Uma matriz de cadeias de caracteres de par chave-valor atribuídas a recursos associados a esta regra quando restauradas a partir da cópia de segurança.

Type: Mapa de string para string

: obrigatório Não

RuleId

Identifica exclusivamente uma regra usada para agendar o backup de uma seleção de recursos.

Type: String

: obrigatório Não

RuleName

Um nome de exibição opcional para uma regra de backup.

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Sim

ScheduleExpression

Uma expressão CRON em UTC especificando quandoAWS BackupInicia um trabalho de backup. Para obter mais informações sobre expressões cron, consulte[Programar expressões para regras](#)noGuia do usuário de Amazon CloudWatch Events.. Antes de especificar um valor para este parâmetro, recomendamos testar sua expressão cron usando um dos muitos geradores cron disponíveis e ferramentas de teste.

Type: String

: obrigatório Não

StartWindowMinutes

Um valor em minutos após um backup ser programado para que um trabalho seja cancelado, se ele não for iniciado com êxito. Este valor é opcional.

Type: Long

: obrigatório Não

targetBackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos para a conta usada para criá-los e oAWSRegião da em que são criadas. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupRuleInput

Especifica uma tarefa programada usada para fazer backup de uma seleção de recursos.

Contents

CompletionWindowMinutes

Um valor em minutos após um trabalho de backup ser iniciado com êxito para que ele seja concluído ou cancelado pelo AWS Backup. Este valor é opcional.

Type: Long

: obrigatório Não

CopyActions

Uma matriz de `CopyAction` objetos, que contém os detalhes da operação de cópia.

Type: Array [CopyAction](#) (p. 374) objects

: obrigatório Não

EnableContinuousBackup

Especifica se o AWS Backup cria backups contínuos. Verdadeiro causa o AWS Backup a criar backups contínuos capazes de PITR (point-in-time restore - restauração point-in-time). Causas falsas (ou não especificadas) o AWS Backup a criar backups de snapshot.

Type: Booleano

: obrigatório Não

Ciclo de vida

O ciclo de vida define quando um recurso protegido é transferido para o armazenamento "frio" e quando ele expira. O AWS Backup fará a transferência e a expiração de 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 "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio".

Tipo: objeto [Lifecycle](#) (p. 378)

: obrigatório Não

RecoveryPointTags

Para ajudar a organizar seus recursos, você pode atribuir seus próprios metadados aos recursos que criar. Cada tag é um par de chave-valor.

Type: Mapa de string para string

: obrigatório Não

RuleName

Um nome de exibição opcional para uma regra de backup.

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Sim

ScheduleExpression

Uma expressão CRON em UTC especificando quandoAWS BackupInicia um trabalho de backup.

Type: String

: obrigatório Não

StartWindowMinutes

Um valor em minutos após um backup ser programado para que um trabalho seja cancelado, se ele não for iniciado com êxito. Este valor é opcional.

Type: Long

: obrigatório Não

targetBackupVaultName

O nome de um contêiner lógico onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos para a conta usada para criá-los e oAWSRegião da em que são criadas. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupSelection

Usado para especificar um conjunto de recursos para um plano de backup.

Contents

IamRoleArn

O ARN da função do IAM que o AWS Backup usa para autenticação ao fazer backup do recurso de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

: obrigatório Sim

ListOfTags

Uma matriz de condições usada para especificar um conjunto de recursos a serem atribuídos a um plano de backup; por exemplo, `"StringEquals": {"ec2:ResourceTag/Department": "accounting"}`. Atribui o plano de backup a todos os recursos com pelo menos uma tag correspondente.

Type: Array [Condition \(p. 373\)](#) objects

: obrigatório Não

Recursos

Uma matriz de strings que contém nomes de recurso da Amazon (ARNs) de recursos a serem atribuídos a um plano de backup.

Type: Matriz de strings

: obrigatório Não

SelectionName

O nome de exibição de um documento de seleção de recursos.

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupSelectionsListMember

Contém metadados sobre umaBackupSelectionObjeto.

Contents

BackupPlanId

Identifica exclusivamente um plano de backup.

Type: String

: obrigatório Não

CreationDate

A data e hora em que um plano de backup é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor deCreationDateé preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

CreatorRequestId

Uma string exclusiva que identifica a solicitação e permite que solicitações com falha sejam repetidas sem o risco de executar a operação duas vezes.

Type: String

: obrigatório Não

IamRoleArn

Especifica a função do IAM nome de recurso da Amazon (ARN) para criar o ponto de recuperação de destino; por exemplo,arn:aws:iam::123456789012:role/S3Access.

Type: String

: obrigatório Não

SelectionId

Identifica exclusivamente uma solicitação para atribuir um conjunto de recursos a um plano de backup.

Type: String

: obrigatório Não

SelectionName

O nome de exibição de um documento de seleção de recursos.

Type: 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 de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupVaultListMember

Contém metadados sobre um cofre de backup.

Contents

BackupVaultArn

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

: 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 para a conta usada para criá-los e o AWS Região da em que são criadas. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Não

CreationDate

A data e hora em que um backup de recurso é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor `1516925490.087` representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

CreatorRequestId

Uma string exclusiva que identifica a solicitação e permite que solicitações com falha sejam repetidas sem o risco de a operação ser executada duas vezes.

Type: String

: 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`.

Type: String

: obrigatório Não

Número de Pontos de Recuperação

O número de pontos de recuperação armazenados em um cofre de backup.

Type: Long

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

CalculatedLifecycle

Contains `DeleteAt` e `MoveToColdStorageAt` carimbos de data/hora, que são usados para especificar um ciclo de vida para um ponto de recuperação.

O ciclo de vida define quando um recurso protegido é passado para armazenamento de baixa atividade e quando expira. AWS Backup o faz com que os backups sejam transferidos e expirados 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 "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS do podem ser transferidos para armazenamento "frio".

Contents

DeleteAt

Um carimbo de data/hora que especifica quando excluir um ponto de recuperação.

Type: Time stamp

: obrigatório Não

MoveToColdStorageAt

Um carimbo de hora que especifica quando migrar um ponto de recuperação para armazenamento "frio".

Type: Time stamp

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

Condition

Contém uma matriz de tripletos composto por um tipo de condição (como `StringEquals`), uma chave e um valor. As condições são usadas para filtrar recursos em uma seleção que é atribuída a um plano de backup.

Contents

ConditionKey

A chave em um par de chave-valor. Por exemplo, em `"ec2:ResourceTag/Department": "accounting"`, `"ec2:ResourceTag/Department"` é a chave.

Type: String

: obrigatório Sim

ConditionType

Uma operação, como `StringEquals`, que é aplicada a um par de chave-valor usado para filtrar recursos em uma seleção.

Type: String

Valores válidos: `STRINGEQUALS`

: obrigatório Sim

ConditionValue

O valor em um par de chave-valor. Por exemplo, em `"ec2:ResourceTag/Department": "accounting"`, `"accounting"` é o valor.

Type: String

: obrigatório Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

CopyAction

Os detalhes da operação de cópia.

Contents

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:vault:aBackupVault`.

Type: String

: obrigatório Sim

Ciclo de vida

Contém uma matriz de `Transition` especificando o tempo, em dias, para que um ponto de recuperação mude para armazenamento "frio" ou seja excluído.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, no console, a configuração de "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS do podem ser transferidos para armazenamento "frio".

Tipo: objeto [Lifecycle](#) (p. 378)

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

CopyJob

Contém informações detalhadas sobre um trabalho de cópia.

Contents

AccountId

O ID da conta da à qual pertence o trabalho de cópia.

Type: String

Padrão: `^[0-9]{12}$`

: obrigatório Não

BackupSizeInBytes

O tamanho, em bytes, de um trabalho de cópia.

Type: Long

: obrigatório Não

CompletionDate

A data e hora em que um trabalho de cópia é concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

CopyJobID

Identificar exclusivamente um trabalho de cópia.

Type: String

: obrigatório Não

CreatedBy

Contém informações sobre o plano de backup e a regra que AWS Backup usado para iniciar o backup do ponto de recuperação.

Tipo: objeto [RecoveryPointCreator](#) (p. 385)

: obrigatório Não

CreationDate

A data e hora em que um trabalho de cópia é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

DestinationBackupVaultArn

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de cópia de destino; por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

: obrigatório Não

DestinationRecoveryPointArn

Um ARN que identifica exclusivamente um ponto de recuperação de destino; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

: obrigatório Não

IamRoleArn

Especifica o ARN da função do IAM usado para copiar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

: obrigatório Não

ResourceArn

O AWSO recurso será copiado; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Type: String

: obrigatório Não

ResourceType

O tipo de AWSO recurso será copiado; por exemplo, um volume do Amazon Elastic Block Store (Amazon EBS) ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Não

sourceBackupVaultARN

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um cofre de cópia de origem, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

: obrigatório Não

SourceRecoveryPointArn

Um ARN que identifica exclusivamente um ponto de recuperação de origem; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

: obrigatório Não

Estado

O estado atual de um trabalho de cópia.

Type: String

Valores válidos: `CREATED` | `RUNNING` | `COMPLETED` | `FAILED`

: obrigatório Não

StatusMessage

Uma mensagem detalhada explicando o status do job para copiar um recurso.

Type: String

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

Lifecycle

Contém uma matriz de `Transition` Especificando o tempo, em dias, para que um ponto de recuperação mude para armazenamento "frio" ou seja excluído.

Os backups transferidos para armazenamento "frio" devem ficar armazenados lá por no mínimo 90 dias. Portanto, no console, a configuração de "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS do podem ser transferidos para armazenamento "frio".

Contents

DeleteAfterDays

Especifica o número de dias após a criação em que um ponto de recuperação é excluído. Deve ser maior que 90 dias mais `MoveToColdStorageAfterDays`.

Type: Long

: obrigatório Não

MoveToColdStorageAfterDays

Especifica o número de dias após a criação em que um ponto de recuperação é movido para armazenamento de baixa atividade.

Type: Long

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

ProtectedResource

Uma estrutura que contém informações sobre um recurso de backup.

Contents

LastBackupTime

A data e hora em que um recurso foi copiado pela última vez, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `LastBackupTime` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

ResourceArn

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um recurso. O formato do ARN depende do tipo de recurso.

Type: String

: obrigatório Não

ResourceType

O tipo de AWS; 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 VSS Windows, o único tipo de recurso com suporte é o Amazon EC2.

Type: 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 de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

RecoveryPointByBackupVault

Contém informações detalhadas sobre os pontos de recuperação armazenados em um cofre de backup.

Contents

BackupSizeInBytes

O tamanho, em bytes, de um backup.

Type: Long

: obrigatório Não

BackupVaultArn

Um ARN que identifica exclusivamente um cofre de backup, por exemplo, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

: 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 para a conta usada para criá-los e o AWS Região da em que são criadas. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Não

Ciclo de vida calculado

A `CalculatedLifecycle` objeto contendo `DeleteAt`, `MoveToColdStorageAt` e `Carimbo` de data/hora.

Tipo: objeto [CalculatedLifecycle](#) (p. 372)

: obrigatório Não

CompletionDate

A data e hora em que um trabalho para restaurar um ponto de recuperação é concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CompletionDate` é preciso para milissegundos. Por exemplo, o valor `1516925490.087` representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

CreatedBy

Contém informações de identificação sobre a criação de um ponto de recuperação, incluindo `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion`, `eBackupRuleId` do plano de backup que é usado para criá-lo.

Tipo: objeto [RecoveryPointCreator](#) (p. 385)

: obrigatório Não

CreationDate

A data e hora em que um ponto de recuperação é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `CreationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: 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`.

Type: String

: obrigatório Não

IamRoleArn

Especifica o ARN da função do IAM usado para criar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

: obrigatório Não

IsEncrypted

Um valor Booleano retornado como `TRUE` se o ponto de recuperação especificado estiver criptografado, ou `FALSE` se o ponto de recuperação não estiver criptografado.

Type: Booleano

: 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` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

Ciclo de vida

O ciclo de vida define quando um recurso protegido é passado para armazenamento de baixa atividade e quando expira. AWS Backup faz com que os backups sejam transferidos e expirados 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 "número de dias para a expiração" deve ser 90 dias maior do que a configuração de "número de dias para transferência ao 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".

Somente os backups do sistema de arquivos do Amazon EFS podem ser transferidos para armazenamento "frio".

Tipo: objeto [Lifecycle \(p. 378\)](#)

: obrigatório Não

RecoveryPointArn

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um ponto de recuperação, por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

: obrigatório Não

ResourceArn

Um ARN que identifica exclusivamente um recurso. O formato do ARN depende do tipo de recurso.

Type: String

: obrigatório Não

ResourceType

O tipo de AWS salvo como um 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 VSS Windows, o único tipo de recurso com suporte é o Amazon EC2.

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Não

sourceBackupVaultARN

O cofre de backup de onde o ponto de recuperação foi originalmente copiado. Se o ponto de recuperação for restaurado para a mesma conta, este valor será `null`.

Type: String

: obrigatório Não

Status

Um código de status que especifica o estado do ponto de recuperação.

Type: String

Valores válidos: `COMPLETED` | `PARTIAL` | `DELETING` | `EXPIRED`

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

RecoveryPointByResource

Contém informações detalhadas sobre um ponto de recuperação salvo.

Contents

BackupSizeBytes

O tamanho, em bytes, de um backup.

Type: Long

: 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 para a conta usada para criá-los e oAWSRegião da em que são criadas. Eles consistem em letras minúsculas, números e hifens.

Type: String

Padrão: `^[a-zA-Z0-9\-_\]{2,50}$`

: obrigatório Não

CreationDate

A data e hora em que um ponto de recuperação é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor deCreationDateé preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: 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`.

Type: String

: obrigatório Não

RecoveryPointArn

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um ponto de recuperação, por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

: obrigatório Não

Status

Um código de status que especifica o estado do ponto de recuperação.

Type: String

Valores válidos: `COMPLETED` | `PARTIAL` | `DELETING` | `EXPIRED`

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

RecoveryPointCreator

Contém informações sobre o plano de backup e a regra que AWS Backup usado para iniciar o backup do ponto de recuperação.

Contents

BackupPlanArn

Um nome de 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`.

Type: String

: obrigatório Não

BackupPlanId

Identifica exclusivamente um plano de backup.

Type: String

: obrigatório Não

BackupPlanVersion

Os IDs de versão são exclusivos gerados aleatoriamente, Unicode, codificadas em UTF-8 que têm no máximo 1.024 bytes. Eles não podem ser editados.

Type: String

: obrigatório Não

BackupRuleID

Identifica exclusivamente uma regra usada para agendar o backup de uma seleção de recursos.

Type: String

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

RestoreJobsListMember

Contém metadados sobre um trabalho de restauração.

Contents

AccountId

O ID da conta da à qual pertence o trabalho de restauração.

Type: String

Padrão: `^[0-9]{12}$`

: obrigatório Não

BackupSizeInBytes

O tamanho, em bytes, do recurso restaurado.

Type: Long

: obrigatório Não

CompletionDate

A data e hora em que um trabalho para restaurar um ponto de recuperação é concluído, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `completionDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

CreatedResourceArn

Um nome de recurso da Amazon (ARN) que identifica exclusivamente um recurso. O formato do ARN depende do tipo de recurso.

Type: String

: obrigatório Não

CreationDate

A data e hora em que um trabalho de restauração é criado, em formato Unix e Tempo Universal Coordenado (UTC). O valor de `creationDate` é preciso para milissegundos. Por exemplo, o valor 1516925490.087 representa sexta-feira, 26 de janeiro de 2018 12:11:30 .087 AM.

Type: Time stamp

: obrigatório Não

ExpectedCompletionTimeMinutes

A quantidade de tempo em minutos que um trabalho restaurando um ponto de recuperação deve levar.

Type: Long

: obrigatório Não

IamRoleArn

Especifica o ARN da função do IAM usado para criar o ponto de recuperação de destino; por exemplo, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

: obrigatório Não

Percentdone

Contém uma porcentagem estimada de conclusão de um trabalho no momento em que o status do job foi consultado.

Type: String

: obrigatório Não

RecoveryPointArn

Um ARN que identifica exclusivamente um ponto de recuperação; por exemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

: 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 VSS Windows, o único tipo de recurso com suporte é o Amazon EC2.

Type: String

Padrão: `^[a-zA-Z0-9\-_\.\]{1,50}$`

: obrigatório Não

RestoreJobid

Identifica exclusivamente o trabalho que restaura um ponto de recuperação.

Type: String

: obrigatório Não

Status

Um código de status especificando o estado do job iniciado pelo AWS Backup para restaurar um ponto de recuperação.

Type: String

Valores válidos: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

: obrigatório Não

StatusMessage

Uma mensagem detalhada explicando o status do trabalho para restaurar um ponto de recuperação.

Type: String

: obrigatório Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos de linguagem, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK para Ruby V3](#)

Erros comuns

Esta seção lista os erros comuns a ações de API de todos AWS Serviços da . 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 atende AWSPadrões.

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

InvalidParameterCombination

Parâmetros que não devem ser usados em conjunto foram usados em conjunto.

Código de status HTTP: 400

InvalidParameterValue

Um valor inválido ou fora do intervalo foi fornecido para o parâmetro de entrada.

Código de status HTTP: 400

InvalidQueryParameter

O AWSA string de consulta da é malformada ou não atende AWSPadrões.

Código de status HTTP: 400

MalformedQueryString

A string de consulta contém um erro de sintaxe.

Código de status HTTP: 404

MissingAction

A solicitação carece de uma ação ou de um parâmetro necessário.

Código de status HTTP: 400

MissingAuthenticationToken

A solicitação deve conter um ID de chave de acesso da AWS válido (registrado) ou um certificado X.509.

Código de status HTTP: 403

MissingParameter

Um parâmetro obrigatório para a ação especificada não foi fornecido.

Código de status HTTP: 400

NãoUTorizado

Você não tem permissão para executar essa 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 deixa de atender às restrições especificadas por umAWSserviçoServiço.

Código de status HTTP: 400

AWSGlossário

Para a mais recente AWS terminologia, consulte o [AWSGlossário](#) no AWS Referência geral.

Histórico de documentos do AWS Backup

A tabela a seguir descreve a documentação desta versão da AWS Backup.

- Versão da API: 2021-04-15
- Última atualização de documentação: 14 de junho de 2021

Alteração	Descrição	Data
Support para backup de vários volumes do Amazon EBS e consistentes com falhas	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 Como criar backup de vários volumes do Amazon EBS e consistentes com falhas .	14 de junho de 2021
Support para o Amazon FSx em adicionais do AWS Regiões	Agora é possível usar o AWS Backup para proteger seus sistemas de arquivos do Amazon FSx nas seguintes regiões: AWS GovCloud (US), Região da Europa (Milão), Região da África (Cidade do Cabo) e Região do Oriente Médio (Bahrein). Para obter mais informações, consulte AWS Backup Endpoints e cotas do AWS Referência geral.	15 de abril de 2021
Support para backups entre regiões e entre contas do Amazon FSX	Agora é possível usar o AWS Backup para copiar backups do Amazon FSX em AWS Regiões e contas. Para obter mais informações, consulte Criar uma cópia de backup . Se você usar políticas gerenciadas pelo cliente, você deve adicionar a nova permissão <code>fsx:CopyBackup</code> para impedir que os trabalhos de backup existentes falhem. Para obter essa permissão, consulte a última declaração na Política	12 de abril de 2021

Alteração	Descrição	Data
	de backup do Amazon FSX na Tabela Política de backup de serviço .	
Support para tags de alocação de custos para backups do Amazon EFS	Agora você pode usar tags de alocação de custo para rastrear custos para seus backups do Amazon EFS em um nível detalhado e visualizar e filtrar essas tags usando AWS Cost Explorer . Para obter mais informações, consulte Como usar tags de alocação de custos .	7 de abril de 2021
Alta autorização do FedRAMP	AWS Backup agora está autorizado a suportar cargas de trabalho FedRAMP High. Para obter mais informações, consulte AWS Serviços no escopo pelo programa de conformidade .	25 de março de 2021
Novo AWS Região	AWS Backup agora está disponível na região Ásia-Pacífico (Osaka). Nesta região, AWS Backup atualmente não suporta AWS Storage Gateway, Amazon FSX e backup entre contas nesta região. Para obter mais informações, consulte AWS Backup Endpoints e cotas do AWS Referência geral.	25 de março de 2021
Support para operações de lote de ponto de recuperação	Agora é possível usar o AWS Backup para automatizar operações em lote para limpar pontos de recuperação em seus cofres de backup. Para obter mais informações, consulte Liberação de recursos .	23 de março de 2021
Support para restaurações para a classe de armazenamento do Amazon EFS One Zone	Agora você pode restaurar seus backups do Amazon EFS para a classe de armazenamento do Amazon EFS One Zone. Para obter mais informações, consulte Restaurar um sistema de arquivos do Amazon EFS .	12 de março de 2021

Alteração	Descrição	Data
Support para restauração point-in-time do Amazon Relational Database Service e backup contínuo	Agora é possível usar o AWS Backup Para automatizar backups contínuos do Amazon RDS e executar restauração pontual (PITR), além de orquestrar backups de snapshots. Para obter mais informações, consulte Recuperação point-in-time .	10 de março de 2021
Support para Amazon CloudWatch e Amazon EventBridge	Agora é possível usar o EventBridge para monitorar AWS Backup eventos e CloudWatch para monitorar AWS Backup Métricas do . Para obter mais informações, consulte Monitorando eventos e métricas com o Amazon CloudWatch e o Amazon EventBridge .	3 de fevereiro de 2021
Support para backups entre contas do	Agora é possível usar o AWS Backup Para fazer backup de seus recursos em várias AWS contas. Para obter mais informações, consulte Backups entre contas .	18 de novembro de 2020
Support para backup e restauração de sistemas de arquivos Amazon FSx	Agora é possível usar o AWS Backup para fazer backup de sistemas de arquivos do Amazon FSx. Para obter mais informações, consulte Trabalhando com sistemas de arquivos do Amazon FSx .	9 de novembro de 2020
Novo AWS Regiões	AWS Backup Agora o está disponível na África (Cidade do Cabo) e Europa (Milão) AWS Regiões. Para obter mais informações, consulte AWS Endpoints e cotas do backup no AWS Referência geral .	21 de outubro de 2020
Support para backup do Windows habilitado para VSS	Agora você pode fazer backup e restaurar aplicativos Windows habilitados para VSS (Volume Shadow Copy Service) em execução em instâncias do Amazon EC2. Para obter mais informações, consulte Criando um Backup do Windows habilitado para VSS .	22 de setembro de 2020

Alteração	Descrição	Data
Support para backup automático do Amazon EFS	Agora é possível usar oAWS BackupPara fazer backup automático de sistemas de arquivos do Amazon EFS. Para obter mais informações, consulte Opção 3: Criar backups automáticos do Amazon EFS .	16 de julho de 2020
NovoAWSRegião	AWS BackupAgora, o está disponível noAWSRegião GovCloud (US). Para obter mais informações, consulte AWSEndpoints e cotas do backup noAWSReferência geral.	24 de junho de 2020
Support para gerenciamento de backups em váriosAWScontas	Agora é possível gerenciar backups em váriosAWScontas do usando o AWS Organizations . Para obter mais informações, consulte Como funciona o gerenciamento entre contas .	24 de junho de 2020
Support para o Amazon Aurora adicionado aoAWSBackup	Agora é possível configurar oAWSBackup para fazer backup de recursos do Amazon Aurora. Para obter mais informações, consulte Visão geral do backup e da restauração de um cluster de banco de dados do Aurora noGuia do usuário do Amazon Aurora.	10 de junho de 2020
Support para configuração de serviços para funcionarem com oAWSBackup	Agora é possível configurar oAWSBackup para backup de recursos do para recursos específicos doAWSServiços da . Para obter mais informações, consulte Configurar serviços para funcionarem com oAWSBackup .	20 de maio de 2020
Support para backup de instâncias do Amazon EC2 e adição de suporte para backup entre regiões do	Agora é possível fazer backup de instâncias do Amazon EC2 do e também copiar recursos do emAWSRegiões. Para obter mais informações, consulte Backup entre regiões .	13 de janeiro de 2020
Novo guia	Esta é a primeira versão do Guia do desenvolvedor do AWS Backup.	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.