Manual do usuário

Amazon EBS

Amazon EBS: Manual do usuário

Table of Contents

O que é o Amazon Elastic Block Store?

O Amazon Elastic Block Store (Amazon EBS) oferece recursos de armazenamento em bloco escaláveis e de alto desempenho que podem ser usados com instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Com o Amazon Elastic Block Store, é possível criar e gerenciar os seguintes recursos de armazenamento em blocos:

- Volumes do Amazon EBS: volumes de armazenamento que são anexados a instâncias do Amazon EC2. Depois de anexar um volume a uma instância, você poderá usá-lo da mesma forma como usaria um disco rígido local conectado a um computador, por exemplo, para armazenar arquivos ou instalar aplicativos.
- Snapshots do Amazon EBS: esses são backups pontuais dos volumes do Amazon EBS que persistem independentemente do volume em si. É possível criar snapshots para fazer backup dos dados nos volumes do Amazon EBS. Em seguida, você poderá restaurar novos volumes desses snapshots a qualquer momento.

Tópicos

Recursos do Amazon EBS

O Amazon EBS fornece os seguintes recursos e benefícios:

- Vários tipos de volume: o Amazon EBS oferece vários tipos de volume que permitem otimizar a performance e o custo do armazenamento para uma ampla variedade de aplicações. Os tipos de volume são divididos em duas categorias principais: armazenamento baseado em SSD para workloads transacionais e em HDD para workloads trabalho de alto throughput.
- Escalabilidade: é possível criar volumes do Amazon EBS com especificações de capacidade e performance que atendam às suas necessidades. À medida que suas necessidades mudam, as operações de volumes elásticos podem ser usadas para aumentar dinamicamente a capacidade ou ajustar a performance, sem causar tempo de inatividade.

- Backup e recuperação: use snapshots do Amazon EBS para fazer backup dos dados armazenados em seus volumes. Em seguida, você pode usar esses snapshots para restaurar volumes instantaneamente ou migrar dados entre contas da AWS, regiões da AWS ou zonas de disponibilidade.
- Proteção de dados: use a criptografia do Amazon EBS para criptografar seus volumes e snapshots do Amazon EBS. As operações de criptografia ocorrem nos servidores que hospedam as instâncias do Amazon EC2, garantindo a segurança dos dados em repouso e dos dados em trânsito entre uma instância e seu volume anexado e snapshots subsequentes.
- Disponibilidade e durabilidade dos dados: os volumes io2 Block Express oferecem 99,999% de durabilidade com uma taxa anual de falhas de 0,001%. Outros tipos de volume oferecem 99,8% a 99,9% de durabilidade com uma taxa anual de falhas de 0,1% a 0,2%. Além disso, os dados dos volumes são replicados em vários servidores em uma zona de disponibilidade para evitar perdas de dados causadas por falha em qualquer componente único.
- Arquivamento de dados: o EBS Snapshots Archive fornece um nível de armazenamento de baixo custo para arquivar cópias completas e pontuais dos snapshots do EBS que você deve reter por 90 dias ou mais por motivos normativos e de conformidade, ou para futuros lançamentos de projetos.

Serviços relacionados

O Amazon EBS funciona com os seguintes serviços:

- Amazon Elastic Compute Cloud: um serviço que permite iniciar e gerenciar máquinas virtuais (instâncias do Amazon EC2) na Nuvem da AWS. É possível anexar volumes do EBS a essas instâncias e usá-las da mesma forma como usaria um disco rígido local conectado, por exemplo, para armazenar arquivos ou instalar aplicações. Para obter mais informações, consulte O que é o Amazon EC2?
- AWS Key Management Service: um serviço gerenciado que permite criar e gerenciar chaves criptográficas. É possível usar chaves criptográficas do AWS KMS para criptografar os dados armazenados nos volumes do Amazon EBS e nos snapshots do Amazon EBS. Para obter mais informações, consulte Como o Amazon EBS usa o AWS KMS.
- Amazon Data Lifecycle Manager: um serviço gerenciado que automatiza a criação, retenção e exclusão de snapshots do EBS e AMIs baseadas no EBS. Você pode usar o Amazon Data Lifecycle Manager para automatizar backups para seus volumes do Amazon EBS e instâncias do Amazon EC2. Para obter mais informações, consulte Amazon Data Lifecycle Manager.

- APIs diretas do EBS: um serviço que permite criar snapshots do EBS, gravar dados diretamente nos snapshots, ler dados nos snapshots e identificar as diferenças ou alterações entre dois snapshots. Para obter mais informações, consulte Usar o APIs diretas do EBS para acessar o conteúdo de um snapshot do EBS.
- Lixeira: um serviço de recurso de recuperação de dados que permite restaurar snapshots do EBS e AMIs baseadas no EBS excluídos acidentalmente. Para obter mais informações, consulte Lixeira.

Acessar o Amazon EBS

É possível criar e gerenciar seus recursos do Amazon ECS usando uma das seguintes interfaces:

Console do Amazon EC2

Uma interface Web para criar e gerenciar volumes e snapshots. Depois de se cadastrar em uma conta da AWS, você pode acessar o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

AWS Command Line Interface

Uma ferramenta de linha de comando que permite gerenciar recursos do Amazon EBS por meio de comandos no shell da linha de comando. É compatível com Windows, Mac e Linux. Para obter mais informações, consulte o Guia do usuário da AWS Command Line Interface e a Referência de comandos da AWS CLI.

AWS Tools for PowerShell

Um conjunto de módulos do PowerShell que ajudam você a programar operações em seus recursos do Amazon EBS usando a linha de comando do PowerShell. Para obter mais informações, consulte o Guia do usuário do AWS Tools for Windows PowerShell e a Referência de comandos do AWS Tools for PowerShell.

AWS CloudFormation

Um serviço da AWS totalmente gerenciado que permite a você criar modelos JSON ou YAML reutilizáveis que descrevem seus recursos da AWS e então provisiona e configura esses recursos para você. Para obter mais informações, consulte o AWS CloudFormationGuia do Usuário.

API de consulta do Amazon EC2

A API de consulta do Amazon EC2 fornece solicitações HTTP ou HTTPS que usam o verbo HTTP `GET` ou `POST` e um parâmetro de consulta chamado `Action`. Para obter mais informações, consulte a Referência da API do Amazon EC2.

SDKs da AWS

APIs específicas de linguagem que permitem criar aplicações integradas aos serviços da AWS. AWS SDKs estão disponíveis para várias linguagens de programação populares. Para obter mais informações, consulte Ferramentas para criar na AWS.

Definição de preço

Com o Amazon EBS, você só paga pelo que provisiona. Para obter mais informações, consulte Definição de preço do Amazon EBS.

Preparação para o Amazon EBS

Conclua as tarefas nesta seção para se preparar para trabalhar com recursos do Amazon EBS.

Tarefas

- Inscreva-se para um Conta da AWS
- Criar um usuário com acesso administrativo
- (Opcional) Crie e use uma chave gerenciada pelo cliente para a criptografia do Amazon EBS
- (Opcional) Habilitar o bloqueio do acesso público aos snapshots do Amazon EBS

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

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

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

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

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso para usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

(Opcional) Crie e use uma chave gerenciada pelo cliente para a criptografia do Amazon EBS

A criptografia do Amazon EBS é uma solução de criptografia que usa chaves AWS KMS criptográficas para criptografar seus volumes e snapshots do Amazon EBS. O Amazon EBS cria automaticamente uma chave KMS AWS gerenciada exclusiva para a criptografia do Amazon EBS em cada região. Essa chave do KMS tem o alias `aws/ebs`. Não é possível fazer a rotação da chave do KMS padrão nem gerenciar suas permissões. Para obter mais flexibilidade e controle sobre a chave do KMS usada na criptografia do Amazon EBS, considere criar e usar uma chave gerenciada pelo cliente.

Para criar e usar uma chave gerenciada pelo cliente para a criptografia do Amazon EBS

1. Crie uma chave do KMS de criptografia simétrica.
2. Selecione a chave do KMS como a chave do KMS padrão para criptografia do Amazon EBS.
3. Conceda aos usuários permissão para usar a chave do KMS para criptografia do Amazon EBS.

(Opcional) Habilitar o bloqueio do acesso público aos snapshots do Amazon EBS

Para evitar o compartilhamento público dos snapshots, você pode habilitar o bloqueio do acesso público aos snapshots. Depois de habilitar o bloqueio do acesso público aos snapshots em uma região, qualquer tentativa de compartilhar publicamente os snapshots nessa região será automaticamente bloqueada. Isso pode ajudar você a melhorar a segurança dos snapshots e a proteger os dados dos snapshots contra acesso não autorizado ou não intencional.

Para ter mais informações, consulte Bloquear o acesso público aos snapshots.

Console

Para habilitar o bloqueio do acesso público aos snapshots

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Painel do EC2 e depois, em Atributos da conta (do lado direito), escolha Proteção e segurança de dados.
3. Na seção Bloquear o acesso público aos snapshots do EBS, escolha Gerenciar.
4. Selecione Bloquear acesso público e depois escolha uma das seguintes opções:
   - Bloquear todos os compartilhamentos: para bloquear todos os compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Além disso, os snapshots que já foram compartilhados publicamente são tratados como privados e não estão mais disponíveis publicamente.
   - Bloquear novos compartilhamentos públicos: para bloquear apenas novos compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Porém, os snapshots que já foram compartilhados publicamente permanecem disponíveis publicamente.
5. Escolha Atualizar.

AWS CLI

Para habilitar o bloqueio do acesso público aos snapshots

Use o comando enable-snapshot-block-public-access. Para `--state`, especifique um dos seguintes valores:

- `block-all-sharing`: para bloquear todos os compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Além disso, os snapshots que já foram compartilhados publicamente são tratados como privados e não estão mais disponíveis publicamente.
- `block-new-sharing`: para bloquear apenas novos compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Porém, os snapshots que já foram compartilhados publicamente permanecem disponíveis publicamente.

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

Volumes do Amazon EBS

Um volume do Amazon EBS é um dispositivo de armazenamento em blocos durável que é possível anexar às suas instâncias. Depois de anexar um volume a uma instância, será possível usá-lo como você usaria um disco rígido físico. Os volumes do EBS são flexíveis. Para volumes de geração atual anexados a tipos de instância de geração atual, é possível aumentar o tamanho dinamicamente, modificar a capacidade de IOPS provisionadas e alterar o tipo de volume em volumes de produção em tempo real.

É possível usar os volumes do EBS como armazenamento principal de dados que exigem atualizações frequentes, como o drive do sistema para uma instância ou armazenamento de uma aplicação de banco de dados. Também é possível usá-los para aplicações com muita throughput que executam verificações de disco contínuas. Os volumes do EBS persistem independentemente da vida útil de uma instância do EC2.

É possível anexar vários volumes do EBS a uma única instância. O volume e a instância devem estar na mesma zona de disponibilidade. Dependendo do volume e dos tipos de instância, você pode usar a opção Anexar várias para montar um volume em várias instâncias ao mesmo tempo.

O Amazon EBS fornece os seguintes tipos de volumes: SSD de uso geral (`gp2` e `gp3`), SSD de IOPS provisionadas (`io1` e `io2`), HDD otimizado para throughput (`st1`), HDD a frio (`sc1`) e Magnético (`standard`). Eles diferem em características de performance e preço, permitindo que você adapte a performance e custo de armazenamento às necessidades das aplicações. Para ter mais informações, consulte Tipos de volume do Amazon EBS.

Sua conta tem um limite no armazenamento total disponível para você. Para obter mais informações sobre esses limites e como solicitar um aumento, consulte Amazon EBS endpoints and quotas.

Para obter mais informações sobre definição de preço, consulte Definição de preço do Amazon EBS.

Tópicos

- Monitorar volumes do Amazon EBS
- Testes de falhas no Amazon EBS

Benefícios de usar volumes do EBS

Os volumes do EBS fornecem benefícios que não são fornecidos por volumes de armazenamento de instâncias.

Benefícios

- Disponibilidade de dados
- Persistência de dados
- Criptografia de dados
- Segurança de dados
- Snapshots
- Flexibilidade

Disponibilidade de dados

Ao criar um volume do EBS, ele será automaticamente replicado na zona de disponibilidade para evitar perda de dados devido à falha de qualquer componente de hardware único. É possível anexar um volume do EBS a qualquer instância do EC2 na mesma zona de disponibilidade. Depois de associar um volume, ele será exibido como um dispositivo de blocos nativo semelhante a um disco rígido ou a outro dispositivo físico. A partir desse momento, a instância pode interagir com o volume da mesma forma que faria com uma unidade local. É possível se conectar à instância e formatar o volume do EBS com um sistema de arquivos, como `Ext4` para uma instância do Linux ou `NTFS` para uma instância do Windows e, em seguida, instalar aplicações.

Se você associar vários volumes a um dispositivo ao qual deu o nome, pode distribuir os dados pelos volumes para maior performance de E/S e throughput.

É possível anexar volumes do EBS `io1` e `io2` para até 16 instâncias baseadas em Nitro. Para obter mais informações, consulte Anexar um volume a várias instâncias com o Multi-Attach do Amazon EBS. Caso contrário, é possível anexar um volume do EBS a uma única instância.

É possível obter dados de monitoramento para seus volumes do EBS, inclusive volumes do dispositivo raiz para instâncias com EBS, sem custo adicional. Para obter mais informações sobre

as métricas de monitoramento, consulte CloudWatch Métricas da Amazon para Amazon EBS. Para obter informações sobre como acompanhar o status de seus volumes, consulte Amazon EventBridge para Amazon EBS.

Persistência de dados

Um volume do EBS é um armazenamento fora da instância capaz de persistir independentemente da duração de uma instância. Você continua a pagar pela utilização do volume, desde que os dados persistam.

Os volumes do EBS que são anexados a uma instância em execução poderão ser desanexados automaticamente da instância com os dados intactos quando a instância for encerrada, se você desmarcar a caixa de seleção Delete on Termination (Excluir no encerramento) ao configurar volumes do EBS para a instância no console do EC2. O volume pode então ser reassociado a uma nova instância, permitindo a rápida recuperação. Se a caixa de seleção de Delete on Termination (Excluir no encerramento) estiver marcada, os volumes serão excluídos no encerramento da instância do EC2. Se você estiver usando uma instância com EBS, poderá pará-la e reiniciá-la sem afetar os dados armazenados no volume associado. O volume permanece associado durante todo o ciclo de parada-início. Isso permite que você processe e armazene os dados no seu volume indefinidamente, usando os recursos de processamento e armazenamento apenas conforme necessário. Os dados persistirão no volume até que o volume seja excluído explicitamente. O armazenamento em bloco físico usado pelos volumes excluídos do EBS é substituído por zeros ou dados criptograficamente pseudoaleatórios antes de ser alocado em um novo volume. Se você estiver lidando com dados confidenciais, deve considerar criptografar seus dados manualmente ou armazenar dados em um volume protegido pelo Criptografia de Amazon EBS. Para ter mais informações, consulte Criptografia do Amazon EBS.

Por padrão, o volume raiz do EBS criado e associado a uma instância em execução é excluído quando essa instância é encerrada. É possível modificar esse comportamento alterando o valor do marcador `DeleteOnTermination` para `false` ao executar a instância. Esse valor modificado faz com que o volume persista mesmo após a instância ser encerrada e permite associar o volume a outra instância.

Por padrão, os volumes adicionais do EBS criados e associados a uma instância em execução não são excluídos quando essa instância é encerrada. É possível modificar esse comportamento alterando o valor do marcador `DeleteOnTermination` para `true` ao executar a instância. Esse valor modificado faz com que o volume seja excluído quando a instância é encerrada.

Criptografia de dados

Para criptografia simplificada de dados, é possível criar volumes do EBS criptografados com o recurso Criptografia de Amazon EBS. Todos os tipos de volume do EBS são compatíveis com criptografia. Você pode usar volumes criptografados do EBS para atender a uma ampla variedade de requisitos de data-at-rest criptografia para dados e aplicativos regulamentados/auditados. A criptografia do Amazon EBS usa algoritmos do Advanced Encryption Standard de 256 bits (AES-256) e uma infraestrutura de chaves gerenciada pela Amazon. A criptografia ocorre no servidor que hospeda a instância do EC2, fornecendo criptografia da instância data-in-transit do EC2 para o armazenamento do Amazon EBS. Para ter mais informações, consulte Criptografia do Amazon EBS.

A criptografia do Amazon EBS é usada AWS KMS keys ao criar volumes criptografados e quaisquer snapshots criados a partir de seus volumes criptografados. Na primeira vez que você cria um volume criptografado do EBS em uma região, uma chave KMS AWS gerenciada padrão é criada automaticamente para você. Essa chave é usada para a criptografia do Amazon EBS, a menos que você crie e use uma chave gerenciada pelo cliente. Criar sua própria chave gerenciada pelo cliente oferece mais flexibilidade, incluindo a capacidade de criar, alternar, desabilitar, definir controles de acesso e auditar as chaves de criptografia usadas para a proteção dos dados. Para mais informações, consulte o Guia do desenvolvedor do AWS Key Management Service.

Segurança de dados

Os volumes do Amazon EBS são apresentados a você como dispositivos de bloco brutos e não formatados. Eles são dispositivos lógicos criados na infraestrutura do EBS, e o serviço Amazon EBS garante que os dispositivos estejam logicamente vazios (ou seja, os blocos brutos são zerados ou contêm dados pseudorrandomizados criptograficamente) antes de qualquer uso ou reutilização por um cliente.

Se você tiver procedimentos que exigem que todos os dados sejam apagados usando um método específico, após ou antes do uso (ou ambos), como aqueles detalhados em DoD 5220,22-M (Manual Operacional do Programa Nacional de Segurança Industrial) ou em NIST 800-88 (Diretrizes para higienização de mídia), será possível fazer isso no Amazon EBS. Essa atividade em nível de bloco será refletida na mídia de armazenamento subjacente dentro do serviço do Amazon EBS.

Snapshots

O Amazon EBS oferece a capacidade de criar snapshots (backups) de qualquer volume do EBS e gravar uma cópia dos dados no volume para o Amazon S3, onde ele é armazenado repetidamente

em várias zonas de disponibilidade. O volume não precisa estar anexado a uma instância em execução para obter um snapshot. À medida que você continua a gravar dados a um volume, pode periodicamente criar um snapshot do volume para usar como linha de base para novos volumes. Esses snapshots podem ser usados para criar vários novos volumes do EBS ou mover volumes entre zonas de disponibilidade. Os snapshots de volumes do EBS criptografados são automaticamente criptografados também.

Ao criar um novo volume a partir de um snapshot, ele será uma cópia exata do volume original no momento em que o snapshot foi tirado. Os volumes do EBS criados de snapshots criptografados são criptografados automaticamente. Ao especificar opcionalmente uma zona de disponibilidade diferente, é possível usar essa funcionalidade para criar uma duplicata do volume nessa zona. Os instantâneos podem ser compartilhados com AWS contas específicas ou tornados públicos. Quando você cria snapshots, são geradas cobranças no Amazon S3 com base no tamanho dos dados cujo backup está sendo feito, não no tamanho do volume de origem. Os snapshots subsequentes do mesmo volume são snapshots incrementais. Eles incluem apenas dados alterados e novos gravados no volume desde a criação do último snapshot, e são geradas cobranças apenas por estes dados alterados e novos.

Snapshots são backups incrementais, o que significa que serão salvos somente os blocos no volume que mudaram depois de o snapshot mais recente. Se você tiver um volume com 100 GiB de dados, mas somente 5 GiB de dados tiverem mudado desde seu último snapshot, somente os 5 GiB de dados modificados serão gravados em Amazon S3. Mesmo que os snapshots sejam salvos de forma incremental, o processo de exclusão de snapshots foi projetado de forma que você precise manter somente o snapshot mais recente.

Para ajudar a categorizar e gerenciar seus volumes e snapshots, é possível marcá-los com os metadados de sua escolha.

Para fazer backup de seus volumes automaticamente, é possível usar Amazon Data Lifecycle Manager ou o AWS Backup.

Flexibilidade

Os volumes do EBS oferecem suporte a alterações de configuração reais durante a produção. É possível modificar o tipo de volume, o tamanho e a capacidade de IOPS sem interrupções de serviço. Para obter mais informações, consulte Modificar um volume do EBS usando Volumes Elásticos do Amazon EBS.

Tipos de volume do Amazon EBS

O Amazon EBS fornece os tipos de volume a seguir, que diferem em características de performance e preço, de forma que você adapte o custo e a performance de armazenamento às necessidades das aplicações.

> **Important**
>
> Há vários fatores que podem afetar a performance dos volumes do EBS, como a configuração da instância, as características de E/S e a demanda das workloads. Para usar totalmente as IOPS provisionadas em um volume do EBS, use instâncias otimizadas para EBS. Para obter mais informações sobre como aproveitar ao máximo seus volumes do EBS, consulte Performance de volumes do Amazon EBS.

Para obter mais informações sobre definição de preço, consulte Definição de preço do Amazon EBS.

Tipos de volume

- Volumes de unidade de estado sólido (SSD)
- Volumes em disco rígido (HDD)
- Volumes da geração anterior

Volumes de unidade de estado sólido (SSD)

Os volumes baseados em SSD são otimizados para workloads de transação envolvendo operações de leitura/gravação frequentes com o tamanho pequeno de E/S, em que o atributo dominante de performance é IOPS. Os tipos de volume baseados em SSD incluem SSD de uso geral e SSD com IOPS provisionadas. A seguir é apresentado um resumo dos casos de uso e características dos volumes baseados em SSD.

	Volumes SSD de uso geral		Volumes de Provisioned IOPS SSD	
Tipo de volume	`gp3`	`gp2`	`io2` Block Express [3]	`io1`
Durabilidade	99,8% a 99,9% de durabilidade (taxa anual de falhas de 0,1% a 0,2%)		Durabilidade de 99,999% (taxa	99,8% a 99,9% de durabilidade (taxa

	Volumes SSD de uso geral		Volumes de Provisioned IOPS SSD	
			anual de falhas de 0,001%)	anual de falhas de 0,1% a 0,2%)
Casos de uso	• Workloads transacionais • Áreas de trabalho virtuais • Bancos de dados de instância única e médio porte • Aplicações interativas de baixa latência • Volumes de inicialização • Ambientes de teste e desenvolvimento		Workloads que exigem: • Latência média abaixo de um milissegundo • Performance estável de IOPS • Mais de 64.000 IOPS ou 1.000 MiB/s de throughput	• Workloads que exigem performance de IOPS sustentado ou mais do que 16.000 IOPS • Workloads de banco de dados com alto consumo de E/S
Tamanho do volume	1 GiB – 16 TiB		4 GiB a 64 TiB [4]	4 GiB – 16 TiB
IOPS máxima por volume	16.000 (64 KiB E/S)	16.000 (16 KiB E/S)	256.000 (16 KiB E/S) [5]	64.000 (16 KiB E/S)
Throughput máxima por volume	1,000 MiB/s	250 MiB/s [1]	4.000 MiB/s	1.000 MiB/s [2]
Multi-attach do Amazon EBS	Sem suporte		Compatível	

	Volumes SSD de uso geral	Volumes de Provisioned IOPS SSD	
Reservas do NVMe	Não compatível	Compatível	Não suportado
Volume de inicialização	Compatível		

[1] O limite de throughput é entre 128 MiB/s e 250 MiB/s, dependendo do tamanho do volume. Para ter mais informações, consulte Performance do volume gp2. Os volumes criados antes de 3 de dezembro de 2018 que não foram modificados desde a criação podem não atingir a performance total, a menos que você modifique o volume.

[2] Para alcançar o throughput máximo de 1.000 MiB/s, o volume deve ser provisionado com 64.000 IOPS e deve ser anexado a instâncias criada no Nitro System. Os volumes criados antes de 6 de dezembro de 2017 que não foram modificados desde a criação podem não alcançar a performance total, a menos que você modifique o volume.

[3] Todos os volumes `io2` criados após 21 de novembro de 2023 são volumes `io2` Block Express. Os volumes `io2` criados antes 21 de novembro de 2023 podem ser convertidos em volumes `io2` Block Express modificando as IOPS ou o tamanho do volume.

[4] volumes com mais de 16 TiB só podem ser anexados a instâncias criadas no Sistema Nitro.

[5] volumes acima de 64.000 IOPS só podem ser anexados a instâncias criadas no Sistema Nitro. Volumes de até 64.000 IOPS podem ser anexados a instâncias não Nitro, mas eles só podem atingir até 32.000 IOPS.

Para obter mais informações sobre os tipos de volume baseados em SSD, consulte o seguinte:

- Volumes SSD de uso geral
- Volumes de Provisioned IOPS SSD

Volumes em disco rígido (HDD)

Os volumes baseados em HDD são otimizados para grandes workloads de streaming em que o atributo de performance dominante é o throughput. Os tipos de volume de HDD incluem HDD com throughput otimizado e HDD frio. A seguir é apresentado um resumo dos casos de uso e características dos volumes baseados em HDD.

	Volumes HDD otimizados para throughput	Volumes HDD a frio
Tipo de volume	`st1`	`sc1`
Durabilidade	99,8% a 99,9% de durabilidade (taxa anual de falhas de 0,1% a 0,2%)	
Casos de uso	• Big data • Data warehouses • Processamento de logs	• Armazenamento orientado para throughput para dados acessados raramente • Cenários nos quais o menor custo de armazenamento é importante
Tamanho do volume	125 GiB – 16 TiB	
Máximo de IOPS por volume (1 MiB E/S)	500	250
Throughput máximo por volume	500 MiB/s	250 MiB/s
Multi-attach do Amazon EBS	Não suportado	
Volume de inicialização	Não suportado	

Para obter mais informações sobre os volumes de unidade de disco rígido (HDD), consulte Volumes de HDD otimizado e HDD frio com throughput.

Volumes da geração anterior

Os volumes magnéticos (`standard`) são volumes da geração anterior apoiados por unidades magnéticas. Eles são adequados para workloads com conjuntos de dados pequenos em que os dados são acessados com pouca frequência e a performance não tem importância primordial. Esses volumes fornecem aproximadamente 100 IOPS em média, com capacidade de expansão de até centenas de IOPS, e podem variar em tamanho de 1 GiB de 1 TiB.

> **Tip**
>
> O volume magnético é um tipo de volume da geração anterior. Se você precisar de desempenho superior ou de uma consistência de desempenho superior à dos volumes da geração anterior, recomendamos que você use um dos mais recentes tipos de volume.

A tabela a seguir descreve os tipos de volumes do EBS de geração anterior.

	Magnético
Tipo de volume	`standard`
Casos de uso	Workloads nas quais os dados são acessados raramente
Tamanho do volume	1 GiB-1 TiB
IOPS máxima por volume	40 a 200
Throughput máximo por volume	40 a 90 MiB/s
Volume de inicialização	Compatível

Para obter mais informações, consulte Volumes da geração anterior.

Volumes SSD de uso geral

Os volumes SSD de uso geral (gp2 e gp3) têm suporte de unidades de estado sólido (SSDs). Eles equilibram preço e performance para proporcionar uma ampla variedade de workloads transacionais. Incluem desktops virtuais, bancos de dados de instâncias únicas de tamanho médio, aplicações interativas sensíveis à latência, ambientes de desenvolvimento e testes e volumes de inicialização. Recomendamos esses volumes para a maioria das workloads.

O Amazon EBS oferece os seguintes tipos de volumes SSD de uso geral:

Tipos

- Volumes SSD de uso geral (gp3)
- Volumes SSD de uso geral (gp2)

Volumes SSD de uso geral (gp3)

Os volumes SSD de uso geral (gp3) são a última geração de volumes SSD de uso geral e o volume SSD com menor custo oferecido pelo Amazon EBS. Esse tipo de volume ajuda a fornecer o equilíbrio certo entre preço e performance para a maioria das aplicações. Também ajuda a escalar a performance do volume independentemente do tamanho do volume. Isso significa que é possível provisionar a performance necessária sem precisar provisionar capacidade adicional de armazenamento em blocos. Além disso, os volumes gp3 oferecem um preço 20% mais baixo por GiB do que os volumes SSD (gp2).

os volumes gp3 fornecem latência de um dígito em milissegundos e durabilidade de volume de 99,8% a 99,9% com uma taxa anual de falhas (AFR) não superior a 0,2%, o que se traduz em um máximo de duas falhas de volume por 1.000 volumes em execução em um período de um ano. AWS projeta volumes gp3 para oferecer seu desempenho provisionado em 99% do tempo.

Conteúdo

- Performance do volume gp3
- Tamanho do volume gp3
- Migrar de gp2 para gp3

Performance do volume gp3

> **Tip**
>
> Os volumes gp3 não usam performance de expansão. Eles conseguem sustentar suas IOPS provisionadas completas e a performance da throughput por tempo indeterminado.

Performance de IOPS

Os volumes gp3 oferecem performance de IOPS consistente de referência de 3.000 IOPS, que está incluído no preço do armazenamento. É possível provisionar IOPS adicionais (até um máximo de 16.000) por um custo adicional a uma proporção de 500 IOPS por GiB de tamanho do volume. O máximo de IOPS pode ser provisionado para volumes de 32 GiB ou mais (500 IOPS por GiB × 32 GiB = 16.000 IOPS).

Performance de throughput

Os volumes gp3 oferecem performance de throughput consistente de referência de 125 MiB/s, que está incluída no preço do armazenamento. É possível provisionar throughput adicional (até um máximo de 1.000 MiB/s) por um custo adicional a uma proporção de 0,25 MiB/s por IOPS provisionadas. A throughput máxima pode ser provisionada a 4.000 IOPS ou superior e a 8 GiB ou maior (4.000 IOPS × 0,25 MiB/s por IOPS = 1.000 MiB/s).

Tamanho do volume gp3

O volume gp3 pode variar de tamanho entre 1 GiB e 16 TiB.

Migrar de gp2 para gp3

Se atualmente estiver usando volumes gp2, você poderá migrar seus volumes para gp3 usando operações Modificar um volume do EBS usando Volumes Elásticos do Amazon EBS. Utilize as operações dos volumes elásticos do Amazon EBS para modificar o tipo de volume, as IOPS e a throughput de seus volumes existentes sem interromper suas instâncias do Amazon EC2. Ao usar o console para criar um volume ou para criar uma AMI a partir de um snapshot, o SSD de uso geral `gp3` é a seleção padrão para tipo de volume. Em outros casos, `gp2` é a seleção padrão. Nesses casos, você pode selecionar `gp3` como o tipo de volume em vez de usar `gp2`.

Para descobrir o quanto você pode economizar ao migrar seus volumes gp2 para gp3, use a calculadora de economia de custos da migração gp2 para gp3 do Amazon EBS.

Volumes SSD de uso geral (gp2)

Oferecem armazenamento com bom custo-benefício, ideal para uma ampla variedade de workloads transacionais. Com volumes gp2, a performance escala conforme o tamanho do volume.

> **Tip**
>
> Os volumes gp3 são a última geração de volumes SSD de uso geral. Oferecem escalabilidade de performance mais previsível e preços até 20% mais baixos do que os volumes gp2. Para ter mais informações, consulte Volumes SSD de uso geral (gp3).
> Para descobrir o quanto você pode economizar ao migrar seus volumes gp2 para gp3, use a calculadora de economia de custos da migração do Amazon EBS gp2 para gp3.

gp2os volumes fornecem latência de um dígito em milissegundos e durabilidade de volume de 99,8% a 99,9% com uma taxa anual de falhas (AFR) não superior a 0,2%, o que se traduz em um máximo de duas falhas de volume por 1.000 volumes em execução em um período de um ano. AWS projeta gp2 volumes para oferecer seu desempenho provisionado em 99% do tempo.

Conteúdo

Performance do volume **gp2**

Performance de IOPS

A performance de referência escala linearmente entre um mínimo de 100 e um máximo de 16.000, a uma taxa de 3 IOPS por GiB de tamanho do volume. A performance das IOPS é provisionada da seguinte forma:

- Volumes de 33,33 GiB e menores são provisionados com o mínimo de 100 IOPS.
- Volumes maiores que 33,33 GiB são provisionados com 3 IOPS por GiB de tamanho do volume até o máximo de 16.000 IOPS, que é atingido em 5.334 GiB (3 x 5.334).
- Volumes de 5.334 GiB e maiores são provisionados com 16.000 IOPS.

Volumes gp2 menores que 1 TiB (e que são provisionados com menos de 3.000 IOPS) podem expandir para 3.000 IOPS, quando necessário, por um período estendido. A capacidade de expansão de um volume é governada por créditos de E/S. Quando a demanda de E/S é maior que a performance de referência, o volume gasta créditos de E/S para atingir o nível de performance necessário (até 3.000 IOPS). Enquanto em intermitência, os créditos de E/S não são acumulados e são gastos na taxa de IOPS que está sendo usada acima do IOPS básico (taxa de gasto = IOPS intermitente - IOPS de linha de base). Quanto mais créditos de E/S o volume tiver acumulado, por mais tempo ele será capaz de sustentar a performance de expansão. Você pode calcular a duração da expansão desta forma:

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

Quando a demanda de E/S cai para o nível de performance de referência ou inferior, o volume começa a obter créditos de E/S a uma taxa de três créditos de E/S por GiB de tamanho do volume por segundo. Os volumes têm um limite de crédito de E/S acumulado de 5,4 milhões de créditos de E/S, que é suficiente para sustentar a performance máxima de expansão de 3.000 IOPS por pelo menos 30 minutos.

> **Note**
>
> Cada volume recebe um saldo de crédito de E/S inicial de 5,4 milhões de créditos de E/S, que fornece um ciclo de inicialização rápido para os volumes de inicialização e uma boa experiência de bootstrap para outras aplicações.

A tabela a seguir apresenta exemplos de tamanhos de volume e a performance de referência associada do volume, a duração da expansão (quando começa com 5,4 milhões de créditos de E/S) e o tempo necessário para preencher novamente um saldo de créditos de E/S vazio.

Tamanho do volume (GiB)	Performance basal (IOPS)	Duração da expansão a 3.000 IOPS (segundos)	Tempo para preencher novamente o saldo de créditos vazio (segundos)
1 a 33,33	100	1,862	54,000

Tamanho do volume (GiB)	Performance basal (IOPS)	Duração da expansão a 3.000 IOPS (segundos)	Tempo para preencher novamente o saldo de créditos vazio (segundos)
100	300	2.000	18.000
334 (tamanho mín. para throughput máx.)	1.002	2.703	5.389
750	2.250	7.200	2.400
1.000	3,000	N/D*	N/D*
5.334 (tamanho mínimo para IOPS máximas) e maior	16.000	N/D*	N/D*

* A performance basal do volume excede a performance de expansão máxima.

Você pode monitorar o saldo de crédito de E/S de um volume usando a `BurstBalance` métrica do Amazon EBS na Amazon. CloudWatch Essa métrica mostra a porcentagem de créditos de E/S para o `gp2` restante. Para ter mais informações, consulte Características e monitoramento de E/S do Amazon EBS. Também é possível definir um alarme que notifica você quando o valor de `BurstBalance` cai para determinado nível. Para obter mais informações, consulte Criação de CloudWatch alarmes.

Performance de throughput

Volumes `gp2` fornecem throughput entre 128 MiB/s e 250 MiB/s, conforme o tamanho do volume. A performance da throughput é provisionada da seguinte forma:

- Volumes de 170 GiB e menores fornecem uma throughput máxima de 128 MiB/s.
- Os volumes maiores que 170 GiB e menores que 334 GiB poderão expandir para uma throughput máxima de 250 MiB/s.
- Volumes de 334 GiB e maiores fornecem 250 MiB/s.

A throughput de um volume gp2 pode ser calculada usando a seguinte fórmula, até o limite de 250 MiB/s de throughput:

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

Tamanho do volume **gp2**

O volume do gp2 pode variar de tamanho entre 1 GiB e 16 TiB. Lembre-se de que a performance do volume é escalada linearmente com o tamanho do volume.

Volumes de Provisioned IOPS SSD

Os volumes SSD de IOPS provisionadas têm suporte de unidades de estado sólido (SSDs). São os volumes de armazenamento do Amazon EBS da mais alta performance, criados para workloads essenciais, com uso intenso de IOPS e de throughput que exigem baixa latência. Os volumes SSD com IOPS provisionadas fornecem a performance provisionada 99,9% do tempo.

O Amazon EBS oferece dois tipos de volumes de SSD com IOPS provisionadas:

- Volumes Block Express de SSD de IOPS provisionadas (io2)
- Volumes de SSD de IOPS provisionadas (io1)

Volumes Block Express de SSD de IOPS provisionadas (**io2**)

Os volumes io2 Block Express se baseiam na última geração de arquitetura de servidor de armazenamento do Amazon EBS. Ela foi criada com o objetivo de atender aos requisitos de performance das aplicações mais exigentes em termos de E/S executadas em instâncias criadas no Nitro System. Com a mais alta durabilidade e a mais baixa latência, o Block Express é ideal para executar workloads de performance intensa críticas para a missão, como o Oracle, o SAP HANA, o Microsoft SQL Server e o SAS Analytics.

A arquitetura Block Express aumenta a performance e a escala dos volumes io2. Os servidores do Block Express se comunicam com as instâncias criadas no Nitro System usando o protocolo de rede Scalable Reliable Datagram (SRD). Essa interface é implementada no Nitro Card dedicado à função de E/S do Amazon EBS no hardware de host da instância. Ela minimiza o atraso de E/S e a variação da latência (tremulação de rede), o que proporciona uma performance mais rápida e consistente para suas aplicações.

Os volumes io2 Block Express foram desenhados para fornecer 99,999% de durabilidade com uma taxa anual de falhas (AFR) não superior a 0,001%, o que significa uma única falha de volume

por 100.000 volumes em execução no período de um ano. Os volumes io2 Block Express são adequados para workloads que se beneficiam de ter um único volume que fornece latência abaixo de um milissegundo, é compatível com IOPS e throughput mais altos, e tem mais capacidade que os volumes gp3.

Os volumes (io2) Block Express de SSD com IOPS provisionadas fornecem a performance provisionada 99,9% do tempo.

Os volumes io2 do Block Express são compatíveis com todas as instâncias criadas no Nitro System. Para obter mais informações, consulte Volumes io2 Block Express.

Tópicos

- Considerações
- Performance

Considerações

- Os volumes io2 Block Express estão disponíveis nas seguintes regiões: Leste dos EUA (Ohio)| Leste dos EUA (Norte da Virgínia) | Oeste dos EUA (N. da Califórnia) | Oeste dos EUA (Oregon) | Ásia-Pacífico (Hong Kong) | Ásia-Pacífico (Mumbai) | Ásia-Pacífico (Seul) | Ásia-Pacífico (Singapura) | Ásia-Pacífico (Sydney) | Ásia-Pacífico (Tóquio) | Canadá (Central) | Europa (Frankfurt) | Europa (Irlanda) | Europa (Londres) | Europa (Estocolmo) | Oriente Médio (Bahrein).
- Todos os volumes io2 criados após 21 de novembro de 2023 são volumes io2 Block Express. Os volumes io2 criados antes 21 de novembro de 2023 podem ser convertidos em volumes io2 Block Express modificando as IOPS ou o tamanho do volume.
- As instâncias criadas no Nitro System podem ser anexadas a volumes de até 64 TiB. Outros tipos de instância podem ser anexados a volumes de até 16 TiB.
- As instâncias criadas no Nitro System podem ser anexadas a volumes provisionados com até 256.000 IOPS. Outros tipos de instância podem ser anexados a volumes provisionados com até 64.000 IOPS, mas podem alcançar até 32.000 IOPS.
- Para criar um volume io2 criptografado com mais de 16 TiB ou mais de 64.000 IOPS a partir de um snapshot não criptografado ou de um snapshot criptografado compartilhado, você deve:
  1. Criar uma cópia criptografada desse snapshot em sua conta
  2. Usar essa cópia do snapshot para criar o volume

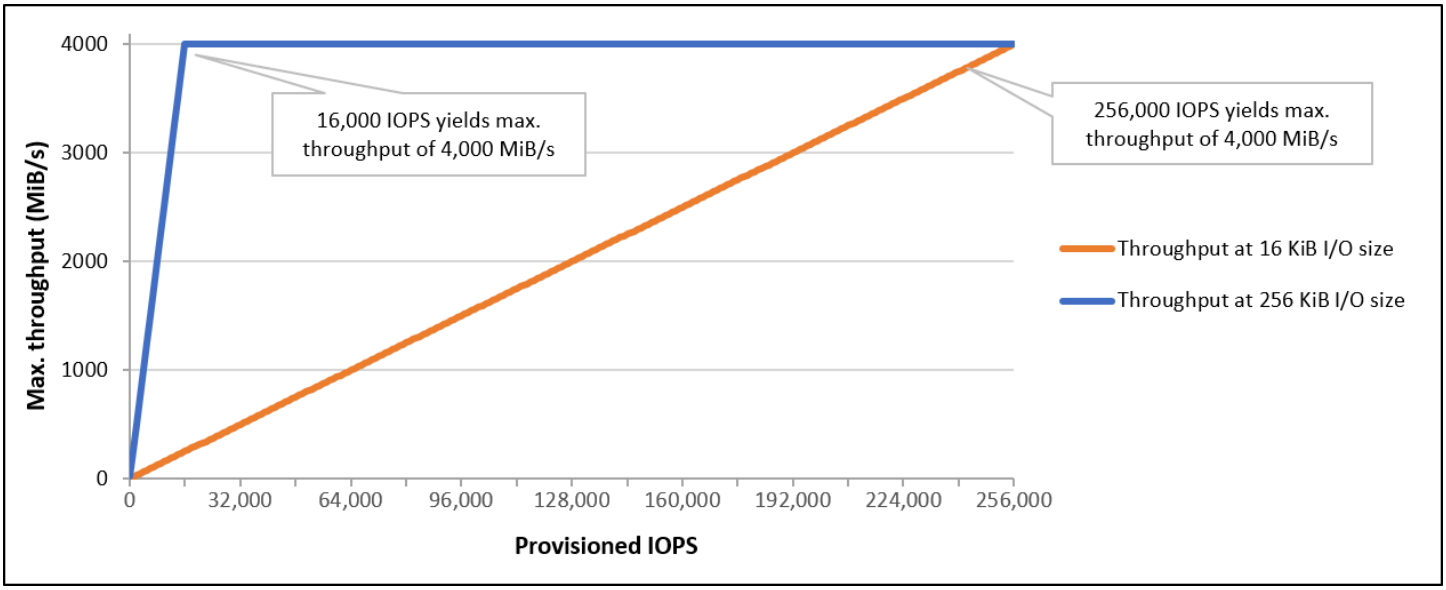
Performance

Com volumes `io2` Block Express, é possível provisionar volumes com:

- Latência média de abaixo de milissegundo
- Capacidade de armazenamento de até 64 TiB (65.536 GiB)
- IOPS provisionadas de até 256.000, com uma relação IOPS:GIB de 1.000:1. As IOPS máximas podem ser provisionadas com volumes de 256 GiB e acima (1.000 IOPS × 256 GiB = 256.000 IOPS).

> **Note**
>
> É possível alcançar até 256.000 IOPS com instâncias criadas no Nitro System. Em outras instâncias, é possível alcançar uma performance de até 32,000 IOPS.

- Throughput de volume de até 4.000 MiB/s. A throughput é dimensionada proporcionalmente até 0,256 MiB/s por IOPS provisionadas. A throughput máxima pode ser alcançada em 16.000 IOPS ou superior.



Volumes de SSD de IOPS provisionadas (`io1`)

Os volumes (`io1`) de SSD com IOPS provisionadas são desenhados para atender às necessidades de workloads com E/S intensa, especialmente workloads de bancos de dados, que são sensíveis a performance e consistência de armazenamento. Os volumes SSD de IOPS provisionadas usam

uma taxa de IOPS consistente, que você especifica ao criar o volume, e o Amazon EBS fornece a performance provisionada em 99,9% do tempo.

Os volumes `io1` são desenhados para fornecer entre 99,8% e 99,9% de durabilidade com uma taxa anual de falhas (AFR) não superior a 0,2 por cento, o que significa uma única falha de volume por 1.000 volumes em execução no período de um ano.

Os volumes `io1` estão disponíveis para todos os tipos de instância do Amazon EC2.

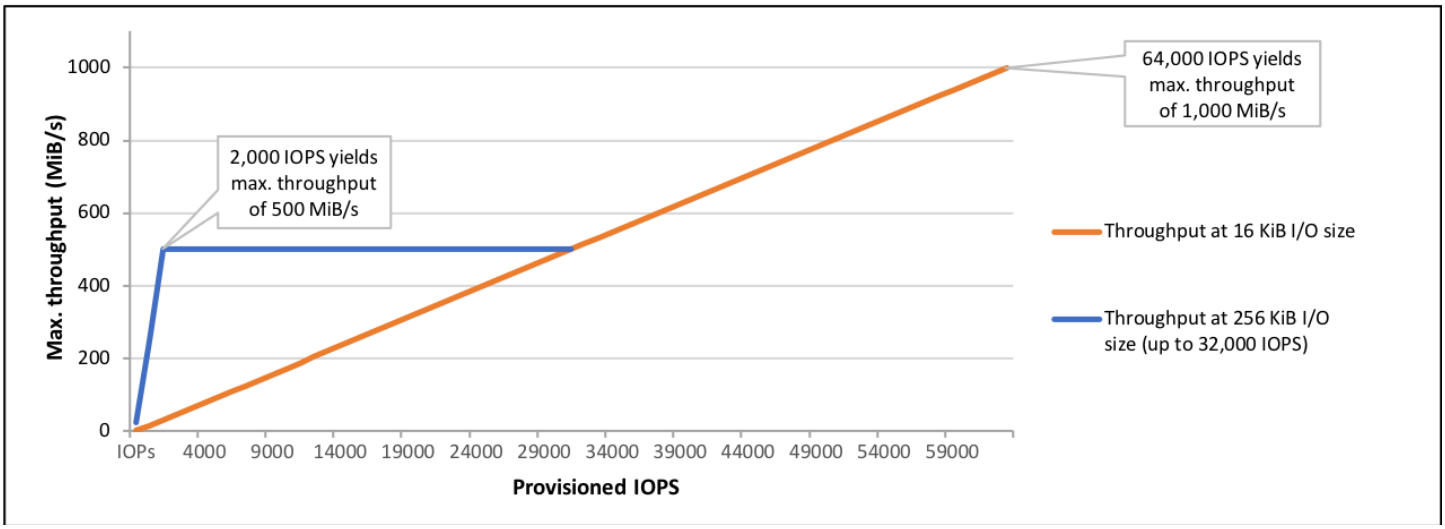
Performance

O tamanho dos volumes `io1` pode variar de 4 GiB a 16 TiB e você pode provisionar de 100 IOPS a 64.000 IOPS por volume. A razão máxima de IOPS provisionadas para o tamanho do volume solicitado (em GiB) é 50:1. Por exemplo, um volume `io1` de 100 GiB pode ser provisionado com até 5.000 IOPS.

As IOPS máximas podem ser provisionadas para volumes de 1.280 GiB ou mais (50 × 1.280 GiB = 64.000 IOPS).

- Os volumes de `io1` provisionados com até 32.000 IOPS oferecem suporte a um tamanho máximo de E/S de 256 KiB e produzem até 500 MiB/s de throughput. Com o tamanho de E/S máximo, o pico da throughput é de 2.000 IOPS.
- Volumes `io1` provisionados com mais de 32.000 IOPS (até o máximo de 64.000 IOPS) geram um aumento linear de throughput a uma taxa de 16 KiB por IOPS provisionada. Por exemplo, um volume provisionado com 48.000 IOPS pode suportar até 750 MiB/s de throughput (16 KiB por IOPS provisionadas × 48.000 IOPS provisionadas = 750 MiB/s).
- Para alcançar a throughput máxima de 1.000 MiB/s, um volume deve ser provisionado com 64.000 IOPS (16 KiB por IOPS provisionadas × 64.000 IOPS provisionadas = 1.000 MiB/s).
- É possível alcançar até 64.000 IOPS em instâncias criadas no Nitro System. Em outras instâncias, é possível alcançar uma performance de até 32,000 IOPS.

. O gráfico a seguir ilustra essas características de performance:



Sua experiência de latência por E/S depende das IOPS provisionadas e do seu perfil de workload. Para obter a melhor experiência de latência de E/S, certifique-se de provisionar IOPS para atender ao perfil de E/S da sua workload.

Volumes de HDD otimizado e HDD frio com throughput

Os volumes com HDD fornecidos pelo Amazon EBS se enquadram nestas categorias:

- HDD otimizado para throughput: um HDD de baixo custo criado para workloads acessadas com frequência e com alta throughput.
- HDD a frio: o design de HDD de menor custo para workloads acessadas com menos frequência.

Tópicos

Limitações na throughput por instância

A throughput dos volumes `st1` e `sc1` sempre é determinado pela menor das seguintes opções:

- Limites de throughput do volume

- Limites de throughput da instância

Quanto a todos os volumes do Amazon EBS, recomendamos selecionar uma instância do EC2 otimizada por EBS adequada para evitar gargalos de rede.

Volumes HDD otimizados para throughput

Os volumes HDD com throughput otimizada (`st1`) fornecem armazenamento magnético de baixo custo que define a performance em termos de throughput, não IOPS. Esse tipo de volume é ideal para workloads grandes e sequenciais, como Amazon EMR, ETL, datas warehouses e processamento de logs. Não há compatibilidade com volumes de `st1` inicializáveis.

Os volumes HDD otimizados para throughput (`st1`), embora semelhantes aos volumes HDD a frio (`sc1`), são projetados para serem compatíveis com dados acessados com frequência.

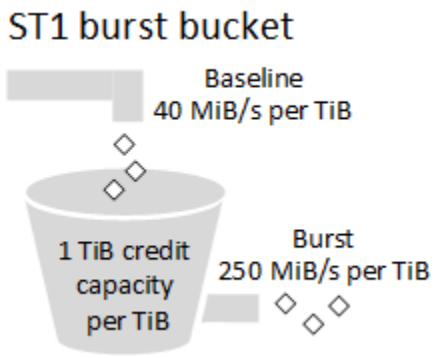
Esse tipo de volume é otimizado para workloads que envolvem E/S sequencial e grande, e recomendamos que clientes com workloads executando E/S pequena e aleatória usem `gp2`. Para ter mais informações, consulte Ineficiência de pequenas leituras/escritas no HDD.

Os volumes de HDD com throughput otimizada (`st1`) anexados a instâncias otimizadas para EBS são concebidos para oferecer performance consistente, proporcionando ao menos 90% da performance esperada de throughput, 99% do tempo em um ano.

Créditos de throughput e performance de expansão

Assim como o `gp2`, o `st1` usa um modelo de bucket de expansão para performance. O tamanho do volume determina a throughput da linha de base do seu volume, que é a taxa na qual o volume acumula créditos de throughput. O tamanho do volume também determina a throughput de expansão do seu volume, que é a taxa em que é possível gastar créditos quando estiverem disponíveis. Os volumes maiores têm throughput basal e de expansão mais altos. Quanto mais créditos seu volume tiver, ele será capaz de acionar E/S da unidade em nível de expansão por mais tempo.

O diagrama a seguir mostra o comportamento do bucket de expansão para `st1`.



Sujeito a throughput e limites de crédito de throughput, a throughput disponível de um volume `st1` é expressada pela seguinte fórmula:

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

Para um volume de `st1` de 1-TiB, a throughput de intermitência está limitada a 250 MiB/s, o bucket se enche com créditos a 40 MiB/s e pode suportar até 1 TiB equivalente em créditos.

Os volumes maiores expandem esses limites de modo linear, com uma throughput máxima de 500 MiB/s. Depois que o bucket se esgota, a throughput é limitada à taxa de base de 40 MiB/s por TiB.

Os tamanhos dos volume variando de 0,125 a 16 TiB, a throughput basal varia de 5 MiB/s até um máximo de 500 MiB/s, que é acessado a 12.5 TiB, da seguinte forma:

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

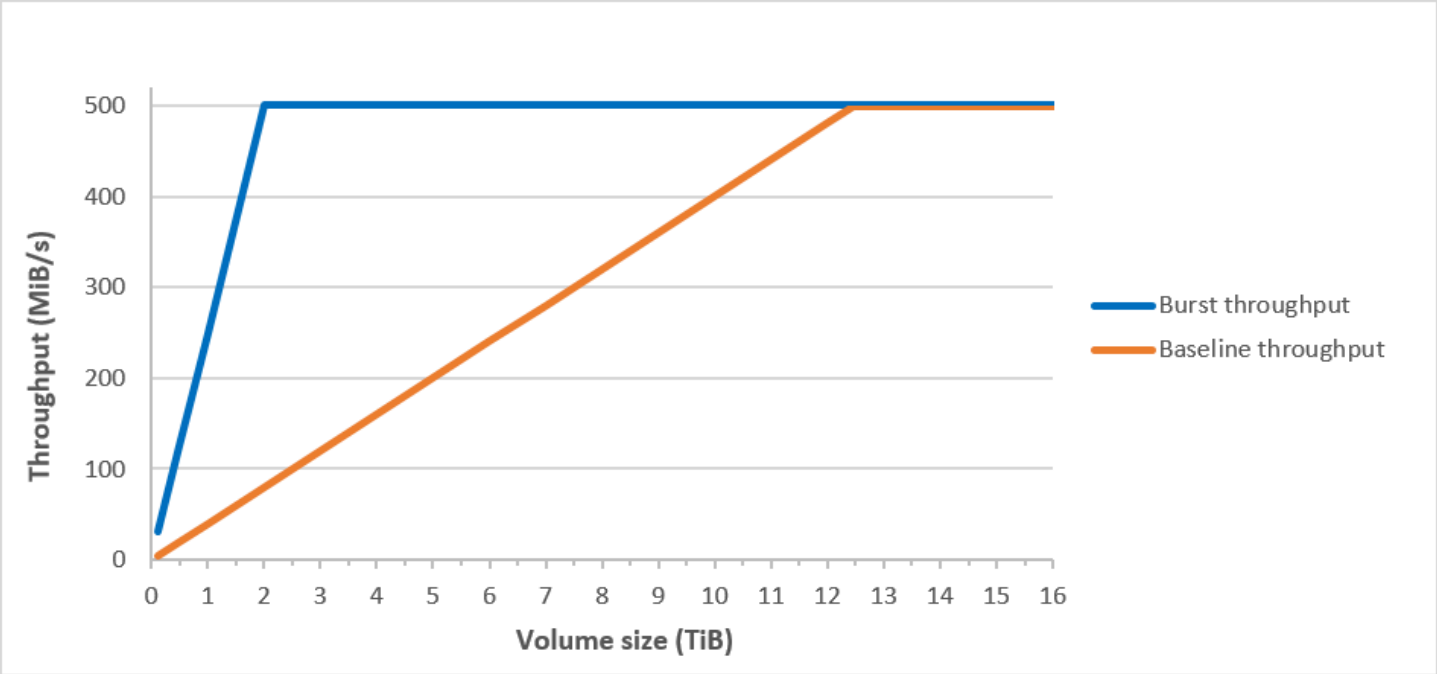
A throughput varia de 31 MiB/s a um limite de 500 MiB/s, que é alcançado em 2 TiB, da seguinte forma:

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

A tabela a seguir apresenta a gama completa de valores de throughput de base e expansão para `st1`.

Tamanho do volume (TiB)	Throughput de base ST1 (MiB/s)	Throughput de expansão do ST1 (MiB/s)
0.125	5	31
0,5	20	125
1	40	250
2	80	500
3	120	500
4	160	500
5	200	500
6	240	500
7	280	500
8	320	500
9	360	500
10	400	500
11	440	500
12	480	500
12,5	500	500
13	500	500
14	500	500
15	500	500
16	500	500

O diagrama a seguir apresenta os valores da tabela:



> **Note**
>
> Quando você cria um snapshot de um volume HDD otimizado para throughput (`st1`), a performance poderá cair até o valor básico do volume enquanto o snapshot estiver em andamento.

Para obter informações sobre o uso de CloudWatch métricas e alarmes para monitorar seu saldo intermitente, consulte. Monitorar o saldo de bucket de expansão para volumes

Volumes HDD a frio

Os volumes de HDD (`sc1`) fornecem armazenamento magnético de baixo custo que define a performance em termos de throughput, não IOPS. Com um limite menor de throughput que `st1`, `sc1` é uma boa opção para workloads grandes, sequenciais e de dados frios. Se você precisar acesso infrequente aos dados e estiver em busca de economia de custos, o `sc1` fornecerá blocos armazenamento econômico. Não há compatibilidade com volumes de `sc1` inicializáveis.

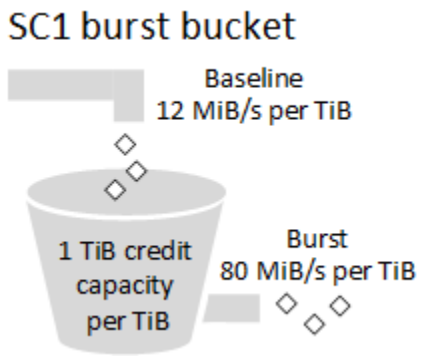
Os volumes HDD a frio (`sc1`), embora similares aos volumes HDD otimizados para throughput (`st1`), são projetados para serem compatíveis com dados acessados com pouca frequência.

> **Note**
>
> Esse tipo de volume é otimizado para workloads que envolvem E/S sequencial e grande, e recomendamos que clientes com workloads executando E/S pequena e aleatória usem `gp2`. Para ter mais informações, consulte Ineficiência de pequenas leituras/escritas no HDD.

Os volumes de HDD frio (`sc1`) anexados a instâncias otimizadas para EBS são concebidos para oferecer performance consistente, proporcionando ao menos 90% da performance esperada de throughput, 99% do tempo em um ano.

Créditos de throughput e performance de expansão

Assim como o `gp2`, o `sc1` usa um modelo de bucket de expansão para performance. O tamanho do volume determina a throughput da linha de base do seu volume, que é a taxa na qual o volume acumula créditos de throughput. O tamanho do volume também determina a throughput de expansão do seu volume, que é a taxa em que é possível gastar créditos quando estiverem disponíveis. Os volumes maiores têm throughput basal e de expansão mais altos. Quanto mais créditos seu volume tiver, ele será capaz de acionar E/S da unidade em nível de expansão por mais tempo.



Sujeito a throughput e limites de crédito de throughput, a throughput disponível de um volume `sc1` é expressada pela seguinte fórmula:

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

Para um volume de `sc1` de 1-TiB, a throughput de expansão está limitada a 80 MiB/s, o bucket se enche com créditos a 12 MiB/s e pode suportar até 1 TiB equivalente em créditos.

Os volumes maiores expandem esses limites de modo linear, com uma throughput máxima de 250 MiB/s. Depois que o bucket se esgota, a throughput é limitada à taxa de base de 12 MiB/s por TiB.

Os tamanhos dos volume variando de 0,125 a 16 TiB, a throughput basal varia de 1,5 MiB/s até um máximo de 192 MiB/s, que é acessado a 16 TiB, da seguinte forma:

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

A throughput varia de 10 MiB/s a um limite de 250 MiB/s, que é alcançado em 3.125 TiB, da seguinte forma:

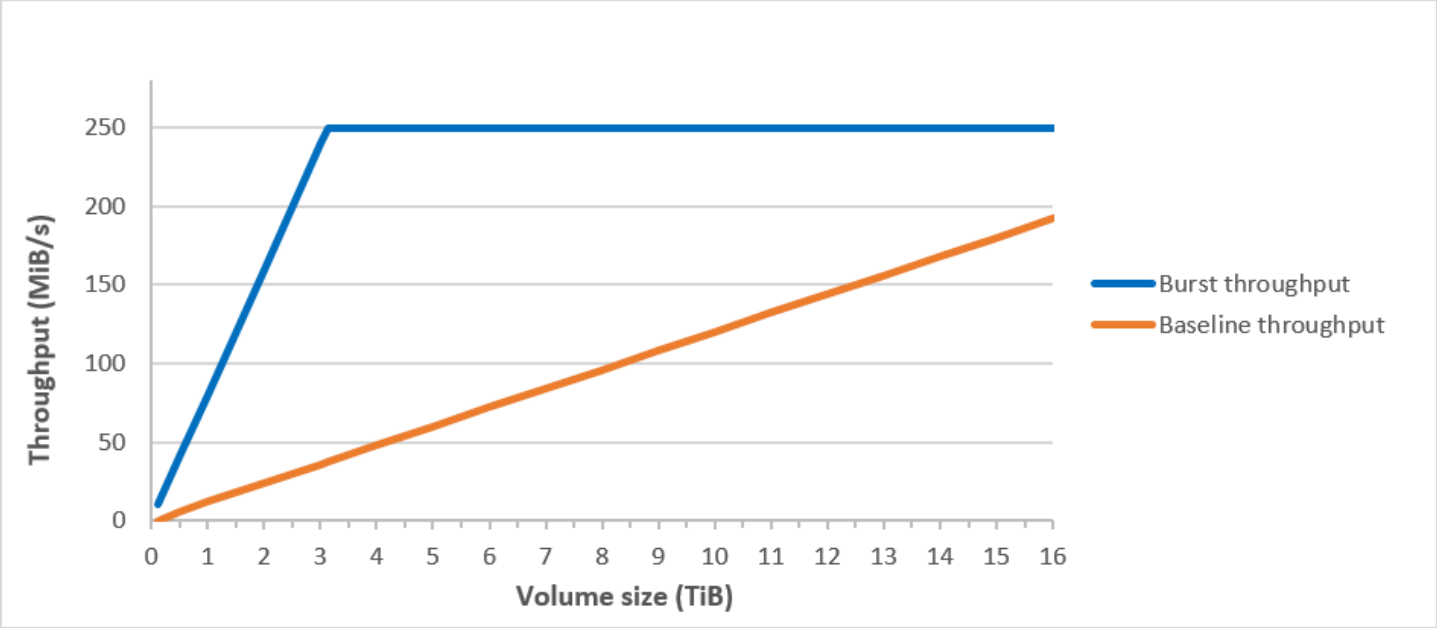
```
             80 MiB/s
3.125 TiB × ----------- = 250 MiB/s
              1 TiB
```

A tabela a seguir apresenta a gama completa de valores de throughput e intermitência para `sc1`:

Tamanho do volume (TiB)	Throughput de base SC1 (MiB/s)	Throughput de expansão do SC1 (MiB/s)
0.125	1.5	10
0,5	6	40
1	12	80
2	24	160
3	36	240
3.125	37.5	250
4	48	250
5	60	250
6	72	250
7	84	250
8	96	250

Tamanho do volume (TiB)	Throughput de base SC1 (MiB/s)	Throughput de expansão do SC1 (MiB/s)
9	108	250
10	120	250
11	132	250
12	144	250
13	156	250
14	168	250
15	180	250
16	192	250

O diagrama a seguir apresenta os valores da tabela:



> **Note**
>
> Quando você cria um snapshot de um volume HDD a frio (`sc1`), a performance pode cair até o valor básico do volume enquanto o snapshot está em andamento.

Para obter informações sobre o uso de CloudWatch métricas e alarmes para monitorar seu saldo intermitente, consulte. Monitorar o saldo de bucket de expansão para volumes

Considerações sobre a performance ao usar volumes de HDD

Para resultados ideais de throughput usando volumes de HDD, planeje suas workloads com as seguintes considerações em mente.

Comparar HDD otimizado para throughput e HDD a frio

Os tamanhos de bucket `st1` e `sc1` variam de acordo com o tamanho do volume, e um bucket completo contém tokens suficientes para uma varredura de volume completa. Contudo, volumes de `st1` e `sc1` maiores demoram mais tempo para a varredura do volume ser concluída, por causa dos limites de throughput por instância e por volume. Os volumes associados a instâncias menores são limitados à throughput por instância em vez de aos limites de throughput de `st1` ou `sc1`.

`st1` e `sc1` são projetados para consistência de performance de 90% de throughput de expansão em 99% do tempo. Os períodos não compatíveis são distribuídos com uniformidade aproximada, destinando 99% da throughput total esperada a cada hora.

Geralmente, os tempos de varredura são expressados por esta fórmula:

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

Por exemplo, levando em conta as garantias de consistência da performance e outras otimizações, pode-se esperar que um cliente de `st1` com volume de 5-TiB conclua uma varredura de volume completa entre 2,91 e 3,27 horas.

- Tempo de varredura ideal

```
   5 TiB            5 TiB
----------- = ------------------ = 10,486 seconds = 2.91 hours
```

```
 500 MiB/s     0.00047684 TiB/s
```

- Tempo máximo de varredura

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

Da mesma forma, um cliente de `sc1` com volume de 5-TiB pode esperar concluir uma varredura de volume completa em 5,83 a 6,54 horas.

- Tempo de varredura ideal

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

- Tempo máximo de varredura

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

A tabela a seguir mostra o tempo de varredura ideal de volumes de vários tamanhos, pressupondo buckets cheios e throughput de instância suficiente.

Tamanho do volume (TiB)	Tempo de varredura de ST1 com expansão (horas) *	Tempo de varredura de SC1 com expansão (horas) *
1	1.17	3.64
2	1.17	3.64
3	1.75	3.64
4	2.33	4.66
5	2.91	5.83

Tamanho do volume (TiB)	Tempo de varredura de ST1 com expansão (horas) *	Tempo de varredura de SC1 com expansão (horas) *
6	3.50	6.99
7	4.08	8.16
8	4.66	9.32
9	5.24	10.49
10	5.83	11.65
11	6.41	12.82
12	6.99	13.98
13	7.57	15.15
14	8.16	16.31
15	8.74	17.48
16	9.32	18.64

* Esses tempos de digitalização pressupõem uma profundidade média de fila (arredondada para o número inteiro mais próximo) de quatro ou mais ao executar 1 MiB de E/S sequencial.

Portanto, se você tiver uma workload orientada para throughput que precise concluir rapidamente digitalizações (até 500 MiB/s) ou exige várias digitalizações de volume completo por dia, use `st1`. Se você estiver otimizando para custo, seus dados são acessados com relativa pouca frequência e você não precisar mais de 250 MiB/s de performance da digitalização, use o `sc1`.

Ineficiência de pequenas leituras/escritas no HDD

O módulo de performance para os volumes `st1` e `sc1` é otimizado para E/Ss sequenciais, favorecendo workloads de alta throughput, oferecendo performance aceitável em workloads com IOPS e throughput mistos e desincentivando workloads com E/S pequena e aleatória.

Por exemplo, uma solicitação de E/S de 1 MiB ou menos conta como um 1 de MiB crédito de E/S. Contudo, se as E/Ss forem sequenciais, elas serão fundidas em blocos de 1 MiB de E/S e contarão somente com 1 MiB de crédito de E/S.

Monitorar o saldo de bucket de expansão para volumes

Você pode monitorar o nível de intermitência do bucket `st1` e os `sc1` volumes usando a `BurstBalance` métrica do Amazon EBS disponível na Amazon. CloudWatch Essa métrica mostra os créditos de throughput para `st1` e `sc1` restantes no bucket de expansão. Para obter mais informações sobre a `BurstBalance` métrica e outras métricas relacionadas à E/S, consulteCaracterísticas e monitoramento de E/S do Amazon EBS. CloudWatch também permite que você defina um alarme que o notifica quando o `BurstBalance` valor cai para um determinado nível. Para obter mais informações, consulte Criação de CloudWatch alarmes.

Restrições de tamanho e configuração de um volume do EBS

O tamanho de um volume do Amazon EBS é limitado pela física e aritmética do armazenamento de dados em bloco, bem como pelas decisões de implementação dos projetistas do sistema operacional (SO) e do sistema de arquivos. AWS impõe limites adicionais ao tamanho do volume para salvaguardar a confiabilidade de seus serviços.

As seções a seguir descrevem os fatores mais importantes que limitam o tamanho utilizável de um volume do EBS e oferecem recomendações para configurar seus volumes do EBS.

Tópicos

Capacidade de armazenamento

A tabela a seguir resume as capacidades de armazenamento teóricas e implementadas para a maioria dos sistemas de arquivos usados comumente no Amazon EBS, presumindo um tamanho de bloco de 4.096 bytes.

Esquema de particionamento	Max. de blocos endereçáveis	Tamanho máx. teórico (blocos × tamanho dos blocos)	Tamanho máx. implementado do Ext4*	Tamanho máx. implementado do XFS**	Tamanho máx. implementado do NTFS	Suporte máx. pelo EBS
MBR	2^{32}	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB
GPT	2^{64}	64 ZiB	1 EiB = 1024^2 TiB (50 TiB certificados em RHEL7)	500 TiB (Certificado na RHEL7)	256 TiB	64 TiB †

* https://ext4.wiki.kernel.org/index.php/Ext4_Howto e https://access.redhat.com/solutions/1532

** https://access.redhat.com/solutions/1532

† Os volumes `io2` Block Express oferecem suporte para até 64 TiB para partições GPT. Para ter mais informações, consulte Volumes Block Express de SSD de IOPS provisionadas (`io2`).

Limitações do serviço

O Amazon EBS abstrai o armazenamento massivamente distribuído de um datacenter em unidades de disco rígido virtuais. Para um sistema operacional instalado em uma instância do EC2, um volume do EBS anexado é exibido como uma unidade de disco rígido virtual contendo setores de disco de 512 bytes. O sistema operacional gerencia a alocação de blocos de dados (ou clusters) nos setores virtuais com os utilitários de gerenciamento de armazenamento. A alocação está em conformidade com um esquema de particionamento de volume, como o registro mestre de inicialização (MBR) ou a tabela de partição do GUID (GPT), e nas capacidades de sistema de arquivos instalado (ext4, NTFS, etc.).

O EBS não considera dados contidos nos setores do disco virtual. Ele garante apenas a integridade dos setores. Isso significa que AWS as ações e as ações do sistema operacional são independentes umas das outras. Ao selecionar um tamanho de volume, lembre-se dos recursos e dos limites de ambos, como nos seguintes casos:

- Atualmente, o EBS oferece suporte a um tamanho máximo de volume de 64 TiB. Isso significa que é possível criar um volume do EBS de até 64 TiB, mas se o sistema operacional reconhecerá toda essa capacidade dependerá de suas próprias características de projeto e de como o volume está dividido.
- Os volumes de inicialização devem usar o esquema de particionamento MBR ou GPT. A AMI da qual uma instância é executada determina o parâmetro do modo de inicialização e, posteriormente, o esquema de partição usado para o volume de inicialização.

  Com o MBR, os volumes de inicialização são limitados a 2 TiB de tamanho.

  Com o GPT, os volumes de inicialização podem ter até 64 TiB quando usados com o modo de inicialização GRUB2 (Linux) ou UEFI (Windows).

  Para ter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso.
- Os volumes de não inicialização com 2 TiB (2.048 GiB) ou mais devem usar uma tabela de partição GPT para acessar todo o volume.

Esquemas de particionamento

Entre outros impactos, o esquema de particionamento determina quantos blocos de dados lógicos podem ser endereçados exclusivamente em um único volume. Para obter mais informações, consulte Tamanhos de blocos de dados. Os esquemas comuns de particionamento em uso são registro mestre de inicialização (MBR) e tabela de partição GUID (GPT). As diferenças importantes entre esses esquemas podem ser resumidas da seguinte forma:

MBR

A MBR usa uma estrutura de dados de 32 bits para armazenar endereços de blocos. Isso significa que cada bloco de dados está mapeado com um de 2^{32} números inteiros possíveis. O tamanho endereçável máximo de um volume é determinado pela fórmula a seguir:

```
2^32 × Block size
```

O tamanho de bloco para volumes MBR normalmente é limitado a 512 bytes. Portanto:

```
2^32 × 512 bytes = 2 TiB
```

As ações alternativas de engenharia para aumentar o limite de 2 TiB para volumes MBR não alcançou a adoção em todo o setor. Consequentemente, o Linux e o Windows nunca detectam um volume MBR como sendo maior que 2 TiB, AWS mesmo que mostrem que seu tamanho é maior.

GPT

A GPT usa uma estrutura de dados de 64 bits para armazenar endereços de blocos. Isso significa que cada bloco de dados está mapeado com um de 2^{64} números inteiros possíveis. O tamanho endereçável máximo de um volume é determinado pela fórmula a seguir:

```
2^64 × Block size
```

O tamanho de bloco para volumes GPT normalmente é de 4.096 bytes. Portanto:

```
2^64 × 4,096 bytes
   = 2^64 × 2^12 bytes
   = 2^70 × 2^6 bytes
   = 64 ZiB
```

Os sistemas de computadores do mundo real não são compatíveis com nada próximo desse máximo teórico. O tamanho do sistema de arquivos implementado está limitado atualmente a 50 TiB para ext4 e a 256 TiB para NTFS.

Tamanhos de blocos de dados

O armazenamento físico de dados em um disco rígido moderno é controlado pelo endereçamento de blocos lógicos, uma camada de abstração que permite que o sistema operacional leia e grave dados em blocos lógicos sem saber muito sobre o hardware subjacente. O sistema operacional depende do dispositivo de armazenamento para mapear os blocos para seus setores físicos. O EBS anuncia setores de 512 bytes para o sistema operacional, que lê e grava dados no disco usando blocos de dados que são um múltiplo do tamanho do setor.

Atualmente, o tamanho padrão do setor para blocos de dados lógico é de 4.096 bytes (4 KiB). Como determinadas workloads se beneficiam de um tamanho de bloco menor ou maior, os sistemas de arquivos aceitam tamanhos de blocos não padrão que podem ser especificados durante a formatação. Os cenários em que os tamanhos de bloco não padrão devem ser usados estão fora do escopo do tópico, mas a opção de tamanho de bloco tem consequências para a capacidade de armazenamento do volume. A tabela a seguir mostra a capacidade de armazenamento como uma função do tamanho do bloco:

Tamanho de bloco	Tamanho máx. do volume
4 KiB (padrão)	16 TiB
8 KiB	32 TiB
16 KiB	64 TiB
32 KiB	128 TiB
64 KiB (máximo)	256 TiB

O limite imposto pelo EBS no tamanho do volume (64 TiB) atualmente é igual ao tamanho máximo permitido pelos blocos de dados de 16 KiB.

Amazon EBS e NVMe

Os volumes do EBS são expostos como dispositivos de blocos NVMe em instâncias criadas no sistema Nitro.

A orientação sobre a performance do EBS em Detalhes do produto Amazon EBS são válidas, independentemente da interface do dispositivo de blocos.

Instâncias do Linux

Os nomes dos dispositivos são `/dev/nvme0n1`, `/dev/nvme1n1` e assim por diante. Os nomes de dispositivo que você especifica no mapeamento de dispositivos de blocos são renomeados usando nomes de dispositivo de NVMe (`/dev/nvme[0-26]n1`). O driver do dispositivo de blocos pode atribuir nomes de dispositivos NVMe em uma ordem diferente da especificada para os volumes no mapeamento de dispositivos de blocos.

Instâncias do Windows

Quando você anexa um volume à instância, você inclui um nome de dispositivo para o volume. Esse nome de dispositivo é usado pelo Amazon EC2. O driver do dispositivo de blocos da instância atribui o nome real do volume ao montá-lo, e o nome atribuído pode ser diferente do nome usado pelo Amazon EC2.

Conteúdo

- Instalar ou atualizar o driver NVMe
- Identificar o dispositivo EBS
- Trabalhar com volumes de NVMe do EBS
- Tempo limite de operação de E/S
- Abort command

Instalar ou atualizar o driver NVMe

Para acessar os volumes de NVMe, os drivers de NVMe devem ser instalados. As instâncias podem ser compatíveis com volumes NVMe do EBS, com volumes de armazenamento de instâncias NVMe, com os dois tipos de volumes de NVMe ou com nenhum volume de NVMe. Para obter mais informações, consulte Resumo dos recursos de rede e armazenamento.

Instâncias do Linux

As seguintes AMIs incluem os drivers NVMe necessários:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 ou posterior com kernel `linux-aws`

> **Note**
>
> AWS Os tipos de instância baseados em Graviton exigem o Ubuntu 18.04 ou posterior com kernel `linux-aws`

- Red Hat Enterprise Linux 6.5 ou posterior
- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior

Como confirmar se a instância tem o driver NVMe

É possível confirmar se sua instância tem o driver NVMe usando o comando a seguir.

- Amazon Linux, RHEL, CentOS e SUSE Linux Enterprise Server

  ```
  $ modinfo nvme
  ```

  Se a instância tiver o driver NVMe, o comando retornará informações sobre o driver.
- Amazon Linux 2 e Ubuntu

  ```
  $ ls /sys/module/ | grep nvme
  ```

  Se a instância tiver o driver NVMe, o comando retornará os drivers instalados.

Como atualizar o driver NVMe

Se sua instância tiver o driver NVMe, será possível atualizar o driver para a versão mais recente usando o procedimento a seguir.

1. Conecte-se à sua instância.
2. Atualize o cache de pacotes para obter as atualizações de pacotes necessárias da seguinte forma:

   - Para Amazon Linux 2, Amazon Linux, CentOS e Red Hat Enterprise Linux:

     ```
     [ec2-user ~]$ sudo yum update -y
     ```

   - Para Ubuntu e Debian:

     ```
     [ec2-user ~]$ sudo apt-get update -y
     ```
3. Ubuntu 16.04 ou posterior incluem o pacote `linux-aws`, que contém os drivers NVMe e ENA exigidos pelas instâncias baseadas em Nitro. Atualize o pacote `linux-aws` para receber a versão mais recente da seguinte forma:

   ```
   [ec2-user ~]$ sudo apt-get install --only-upgrade -y linux-aws
   ```

   Para o Ubuntu 14.04, é possível instalar o pacote mais recente `linux-aws` da seguinte maneira:

   ```
   [ec2-user ~]$ sudo apt-get install linux-aws
   ```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.

Instâncias do Windows

As AMIs AWS do Windows para Windows Server 2008 R2 e versões posteriores incluem o driver AWS NVMe. Se você não estiver usando as AMIs mais recentes AWS do Windows fornecidas pela Amazon, consulte Instalar ou atualizar drivers AWS NVMe usando PowerShell no Guia do usuário do Amazon EC2.

Identificar o dispositivo EBS

O EBS usa virtualização de E/S de raiz única (SR-IOV - single-root I/O virtualization) para fornecer anexos de volume em instâncias baseadas em Nitro usando a especificação NVMe. Esses dispositivos dependem dos drivers NVMe padrão no sistema operacional. Normalmente, esses drivers descobrem dispositivos anexados durante a inicialização da instância e cria nós de dispositivo com base na ordem em que os dispositivos respondem, e não em como os dispositivos são especificados no mapeamento de dispositivos de blocos.

Instâncias do Linux

No Linux, os nomes de dispositivos NVMe seguem o padrão `/dev/nvme<x>n<y>`, em que **<x>** é a ordem de enumeração e, para o EBS, **<y>** é igual a 1. Ocasionalmente, os dispositivos podem responder à descoberta em uma ordem diferente em inicializações subsequentes da instância, o que faz com que o nome do dispositivo seja alterado. Além disso, o nome de dispositivo atribuído pelo driver de dispositivo de bloco pode ser diferente do nome especificado no mapeamento de dispositivos de blocos.

Recomendamos que você use identificadores estáveis para seus volumes do EBS em sua instância, como um dos seguintes:

- Para instâncias baseadas em Nitro, os mapeamentos de dispositivos de blocos especificados no console do Amazon EC2, quando você está anexando um volume do EBS ou durante chamadas à API `AttachVolume` ou `RunInstances`, são capturados no campo de dados específico ao fornecedor da identificação do controlador NVMe. Com as AMIs do Amazon Linux posteriores à

versão 2017.09.01, fornecemos uma regra `udev` que lê esses dados e cria um link simbólico para o mapeamento de dispositivos de blocos.

- O ID do volume do EBS e o ponto de montagem são estáveis entre as alterações de estado da instância. O nome do dispositivo NVMe pode mudar, dependendo da ordem em que os dispositivos respondem durante a inicialização da instância. Recomendamos usar o ID do volume do EBS e o ponto de montagem para a identificação consistente do dispositivo.
- Os volumes do EBS do NVMe têm o ID do volume do EBS definido como o número de série na identificação do dispositivo. Use o comando `lsblk -o +SERIAL` para listar o número de série.
- O formato de nome do dispositivo NVMe pode variar dependendo se o volume do EBS foi anexado durante ou após o lançamento da instância. Os nomes de dispositivos NVMe para volumes anexados após o lançamento da instância incluem o prefixo `/dev/`, enquanto os nomes de dispositivos NVMe para volumes anexados durante o lançamento da instância não incluem o prefixo `/dev/`. Se você estiver usando um Amazon Linux ou FreeBSD AMI, use o comando `sudo ebsnvme-id /dev/nvme0n1 -u` para ter um nome de dispositivo NVMe consistente. Para outras distribuições, use o `sudo nvme id-ctrl -v /dev/nvme0n1` para determinar o nome do dispositivo NVMe.
- Quando um dispositivo é formatado, um UUID é gerado que persiste durante a vida do sistema de arquivos. Um rótulo de dispositivo pode ser especificado ao mesmo tempo. Para obter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso e Inicialização com o volume errado.

Amazon Linux AMIs

Com a AMI do Amazon Linux 2017.09.01 ou posterior (incluindo o Amazon Linux 2), é possível executar o comando ebsnvme-id da seguinte forma para mapear o nome do dispositivo NVMe para um ID de volume e nome de dispositivo:

O exemplo a seguir mostra o comando e a saída para um volume anexado durante o lançamento da instância. Observe que o nome do dispositivo NVMe não inclui o prefixo `/dev/`.

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

O exemplo a seguir mostra o comando e a saída para um volume anexado após o lançamento da instância. Observe que o nome do dispositivo NVMe inclui o prefixo `/dev/`.

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

Amazon Linux também cria um link simbólico do nome do dispositivo no mapeamento de dispositivos de blocos (por exemplo, `/dev/sdf`), para o nome do dispositivo NVMe.

AMIs do FreeBSD

Começando com o FreeBSD 12.2-RELEASE, é possível executar o comando ebsnvme-id conforme mostrado acima. Passe o nome do dispositivo NVMe (por exemplo, `nvme0`) ou o dispositivo de disco (por exemplo, `nvd0` ou `nda0`). O FreeBSD também cria links simbólicos para os dispositivos de disco (por exemplo, `/dev/aws/disk/ebs/`*`volume_id`*).

Outras AMIs em Linux

Com uma versão do kernel de 4.2 ou posterior, é possível executar o comando nvme id-ctrl da seguinte forma para mapear um dispositivo NVMe para um ID de volume. Primeiro, instale o pacote da linha de comando do NVMe, `nvme-cli`, usando as ferramentas de gerenciamento de pacotes para sua distribuição do Linux. Para obter instruções de download e instalação de outras distribuições, consulte a documentação específica para sua distribuição.

O exemplo a seguir obtém o ID do volume e o nome do dispositivo NVMe para um volume que foi anexado durante o lançamento da instância. Observe que o nome do dispositivo NVMe não inclui o prefixo `/dev/`. O nome do dispositivo está disponível por meio da extensão específica ao fornecedor do controlador NVMe (384:4095 bytes da identificação do controlador):

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

O exemplo a seguir obtém o ID do volume e o nome do dispositivo NVMe para um volume que foi anexado após o lançamento da instância. Observe que o nome do dispositivo NVMe inclui o prefixo `/dev/`.

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme1n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : volabcdef01234567890
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

O comando lsblk lista dispositivos disponíveis e seus pontos de montagem (se aplicável). Isso ajuda você a determinar o nome correto do dispositivo a ser usado. Neste exemplo, `/dev/nvme0n1p1` é montado como o dispositivo raiz e `/dev/nvme1n1` é anexado mas não montado.

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

Instâncias do Windows

Você pode executar o comando **`ebsnvme-id`** para mapear o número do disco do dispositivo NVMe para um ID de volume do EBS e um nome de dispositivo. Por padrão, todos os dispositivos NVMe do EBS estão enumerados. É possível passar um número de disco para enumerar informações de um dispositivo específico. A `ebsnvme-id` ferramenta está incluída nas AMIs mais recentes do Windows Server AWS fornecidas, localizadas em`C:\PROGRAMDATA\AMAZON\Tools`.

Começando com o pacote do driver AWS NVMe, `1.5.0,` a versão mais recente da `ebsnvme-id` ferramenta é instalada pelo pacote do driver. A versão mais recente só está disponível no pacote do driver. O link de download autônomo da ferramenta `ebsnvme-id` não receberá mais atualizações. A última versão disponível por meio do link autônomo é a `1.1.0`, que pode ser baixada usando o link ebsnvme-id.zip para extrair o conteúdo para a sua instância do Amazon EC2, a fim de obter acesso ao `ebsnvme-id.exe`.

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

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

Disk Number: 2
Volume ID: vol-038bd1c629aa125e6
Device Name: xvde

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

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

Trabalhar com volumes de NVMe do EBS

Para formatar e montar um volume de NVMe do EBS, consulte Disponibilizar um volume do Amazon EBS para uso.

Instâncias do Linux

Se você estiver usando o kernel Linux 4.2 ou posterior, qualquer alteração que você fizer no tamanho do volume de um volume de NVMe do EBS será automaticamente refletida na instância. Para os kernels do Linux mais antigos, talvez seja necessário desanexar e anexar o volume do EBS ou reiniciar a instância para que a alteração de tamanho seja refletida. Com o kernel 3.19 ou posterior do Linux, é possível usar o comando hdparm da seguinte forma para forçar uma nova varredura do dispositivo NVMe:

```
[ec2-user ~]$ sudo hdparm -z /dev/nvme1n1
```

Quando você desanexa um volume de NVMe do EBS, a instância não tem a oportunidade de liberar os caches ou metadados do sistema de arquivos antes de desanexar o volume. Portanto, antes de desanexar um volume de NVMe do EBS, você deverá sincronizá-lo e desmontá-lo. Se o volume não for desanexado, tente o comando `force-detach`, conforme descrito em Desanexar um volume do Amazon EBS de uma instância.

Instâncias do Windows

As AMIs mais recentes AWS do Windows contêm o driver AWS NVMe exigido pelos tipos de instância que expõem os volumes do EBS como dispositivos de bloco NVMe. No entanto, se você redimensionar seu volume raiz em um sistema Windows, será necessário fazer a varredura novamente do volume para que a alteração seja refletida na instância. Se você executou sua instância a partir de uma AMI diferente, ela pode não conter o driver AWS NVMe necessário. Se sua instância não tiver o driver AWS NVMe mais recente, você deverá instalá-lo. Para obter mais informações, consulte Drivers do AWS NVMe para instâncias Windows.

Tempo limite de operação de E/S

A maioria dos sistemas operacionais especifica um tempo limite para as operações de E/S enviadas aos dispositivos NVMe.

Instâncias do Linux

No Linux, os volumes do EBS anexados a instâncias baseadas em Nitro usam o driver do NVMe padrão fornecido pelo sistema operacional. A maioria dos sistemas operacionais especifica um tempo limite para as operações de E/S enviadas aos dispositivos NVMe. O tempo limite padrão é de 30 segundos e pode ser alterado usando o parâmetro de inicialização `nvme_core.io_timeout`. Para a maioria dos kernels do Linux anteriores à versão 4.6, esse parâmetro é `nvme.io_timeout`.

Se a latência de E/S exceder o valor desse parâmetro de tempo limite, o driver NVMe do Linux falhará na E/S e retornará um erro ao sistema de arquivos ou à aplicação. Dependendo da operação de E/S, seu sistema de arquivos ou aplicação poderá tentar o erro novamente. Em alguns casos, o sistema de arquivos pode ser remontado como somente leitura.

Para obter uma experiência semelhante à dos volumes do EBS anexados às instâncias do Xen, recomendamos que você configure `nvme_core.io_timeout` como o maior valor possível. Para os kernels atuais, o máximo é 4294967295, enquanto para os kernels anteriores o máximo é 255. Dependendo da versão do Linux, o tempo limite pode já estar definido como o máximo valor possível. Por exemplo, o tempo limite é definido como 4294967295 por padrão para a AMI do Amazon Linux 2017.09.01 e posterior.

É possível verificar o valor máximo de sua distribuição Linux gravando um valor mais alto que o máximo sugerido para `/sys/module/nvme_core/parameters/io_timeout` e verificando se ocorre o erro Resultado numérico fora do intervalo ao tentar salvar o arquivo.

Instâncias do Windows

No Windows, o tempo limite padrão é de 60 segundos e o máximo é de 255 segundos. É possível modificar a configuração de registro de classe de disco `TimeoutValue` usando o procedimento descrito em Entradas de registro para drivers de Miniport de SCSI.

Abort command

`Abort` é um comando Admin do NVMe emitido para cancelar um comando específico enviado anteriormente ao controlador. Esse comando geralmente é emitido pelo driver de dispositivo para dispositivos de armazenamento que excederam o limite de tempo limite da operação de E/S. Tipos de instância do Amazon EC2 compatíveis com o comando `Abort` por padrão anulará um comando específico que foi enviado anteriormente para o controlador do dispositivo Amazon EBS conectado ao qual um comando `Abort` é emitido.

Os tipos de instância a seguir são compatíveis com o comando `Abort` para todos os volumes do Amazon EBS anexados por padrão:`R5b`, `R6i`, `M6i`, `M6a`, `C6gn`, `C6i`, `X2gd`, `X2iezn`, `Im4gn`, `Is4gen`.

Outros tipos de instância não realizam nenhuma ação quando os comandos `Abort` são emitidos para volumes do Amazon EBS anexados.

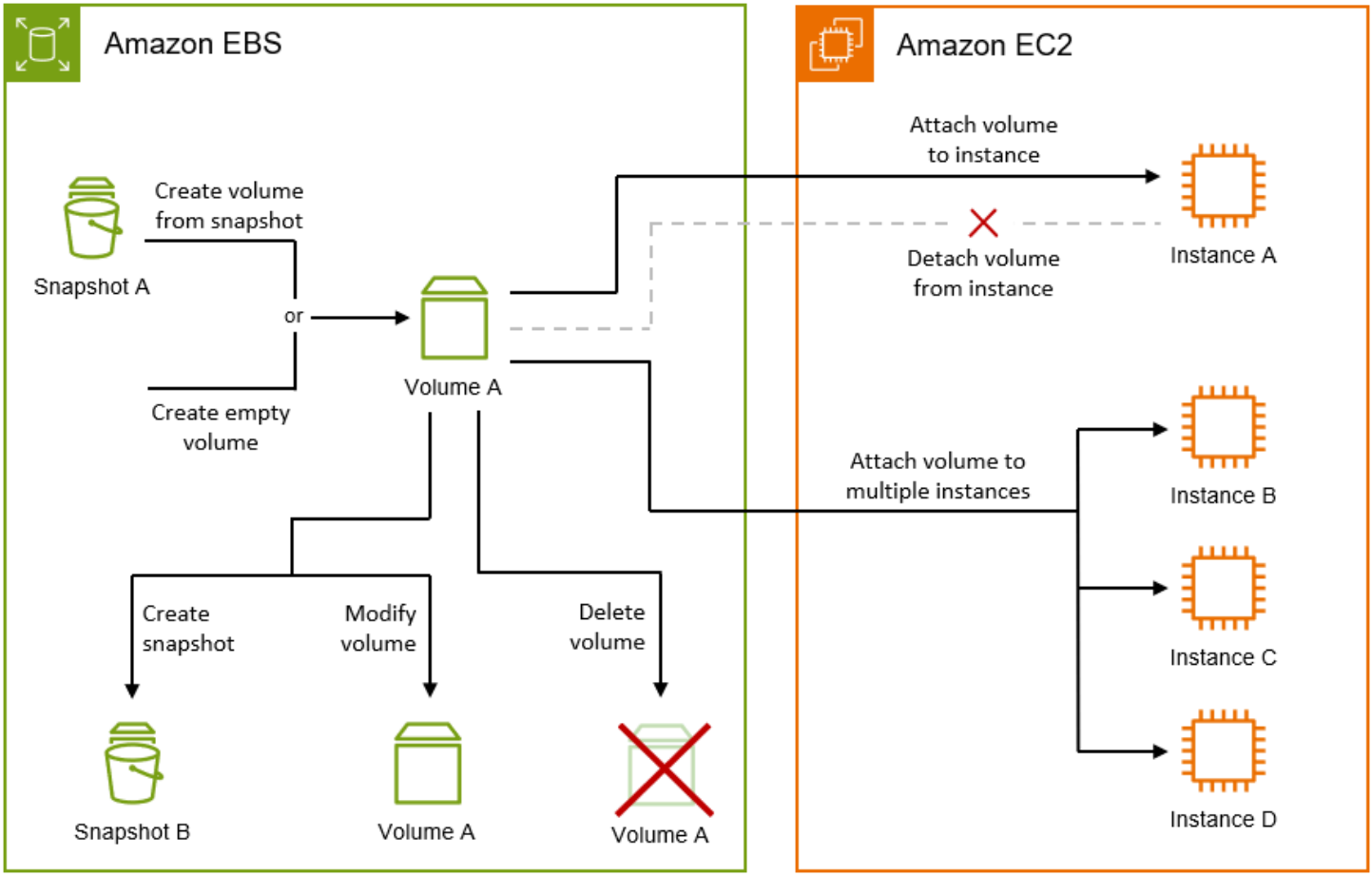
Dispositivos Amazon EBS com versão de dispositivo NVMe `1.4` ou superior são compatíveis com o comando `Abort`.

Para obter mais informações, consulte a seção 5.1 Abort command (Comando anular da NVM Express Base Specification (Especificação da base NVM Express).

Ciclo de vida do volume do Amazon EBS

O ciclo de vida de um volume do Amazon EBS começa com o processo de criação. Você pode criar um volume com base em um snapshot do Amazon EBS ou criar um volume vazio. Antes de usar seu volume, anexe-o a uma ou mais instâncias do Amazon EC2 que estejam na mesma zona de disponibilidade que o volume. É possível anexar vários volumes do EBS a uma única instância. Se necessário, também é possível desanexar um volume de uma instância e, em seguida, anexá-lo a outra instância. Se seus requisitos de armazenamento mudarem, você poderá modificar o tamanho ou a performance do volume a qualquer momento. Você pode criar point-in-time backups dos seus volumes criando snapshots do Amazon EBS. Se não precisar mais de um volume, você poderá excluí-lo para não incorrer nos custos de armazenamento relacionados.

A imagem a seguir mostra as ações que podem ser realizadas em seus volumes como parte do ciclo de vida do volume.



Há também tarefas que você deve executar conectando-se à instância e executando um comando do sistema operacional. Por exemplo, formatar o volume, montar o volume, gerenciar partições e visualizar o espaço livre em disco.

Tarefas

- Crie um volume do Amazon EBS.
- Vincular um volume de Amazon EBS a uma instância
- Anexar um volume a várias instâncias com o Multi-Attach do Amazon EBS
- Disponibilizar um volume do Amazon EBS para uso
- Visualizar informações sobre um volume do Amazon EBS
- Modificar um volume do EBS usando Volumes Elásticos do Amazon EBS
- Desanexar um volume do Amazon EBS de uma instância
- Excluir um volume de Amazon EBS

Crie um volume do Amazon EBS.

É possível criar um volume do Amazon EBS e anexá-lo a qualquer instância do EC2 na mesma zona de disponibilidade. Se você criar um volume do EBS criptografado, só poderá anexá-lo a tipos de instância compatíveis. Para ter mais informações, consulte Tipos de instâncias compatíveis.

Se você estiver criando um volume para um cenário de armazenamento de alta performance, use um volume SSD de IOPS provisionadas (`io1` ou `io2`) e associe-o a uma instância com largura de banda suficiente para oferecer suporte a sua aplicação, como uma instância otimizada para EBS. A mesma orientação se aplica a volumes HDD otimizado para throughput (`st1`) e HDD a frio (`sc1`).

> **Note**
>
> Se você criar um volume para uso com uma instância do Windows e ele tiver mais de 2.048 GiB (ou menos de 2.048 GiB, mas for possível aumentá-lo posteriormente), configure o volume para usar tabelas de partição GPT. Para obter mais informações, consulte Suporte do Windows para discos rígidos maiores que 2 TB..

Os volumes vazios do EBS recebem a performance máxima no momento em que são disponibilizados e não requerem inicialização (antes conhecida como pré-aquecimento). Contudo, os blocos de armazenamento em volumes que foram criados de snapshots devem ser inicializados (extraídos do Amazon S3 e gravados no volume) para é possívelr acessar o bloco. Essa ação preliminar leva tempo e pode causar um aumento significativo na latência de uma operação de E/S na primeira vez que cada bloco é acessado. A performance do volume é obtida depois que todos os blocos forem obtidos por download e gravados no volume. Para a maioria das aplicações, é aceitável amortizar esse custo ao longo da vida útil do volume. Para evitar essa ocorrência de performance inicial em um ambiente de produção, é possível forçar a inicialização imediata de todo o volume ou habilitar a restauração rápida de snapshots. Para obter mais informações, consulte Inicializar volumes de Amazon EBS.

Métodos de criação de um volume

- Crie e anexe volumes do EBS ao executar instâncias especificando um mapeamento de dispositivos de blocos. Para obter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instâncias e Bloquear mapeamentos de dispositivos.
- Crie um volume do EBS e anexe-o a uma instância em execução. Para obter mais informações, consulte Criar um volume vazio abaixo.

- Crie um volume do EBS de um snapshot criado anteriormente e anexe-o a uma instância em execução. Para obter mais informações, consulte Criar um volume a partir de um snapshot abaixo.

Tópicos

Criar um volume vazio

Os volumes vazios recebem sua performance máxima no momento em que estão disponíveis e não exigem inicialização.

É possível criar um volume EBS vazio usando um dos métodos a seguir.

Console

Para criar um volume EBS vazio usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Escolha Create volume (Criar volume).
4. Em Volume type (Tipo de volume), escolha o tipo de volume a ser criado. Para ter mais informações, consulte Tipos de volume do Amazon EBS.

   O SSD `gp3` de uso geral é a seleção padrão.
5. Para Size (Tamanho), informe o tamanho do volume, em GiB. Para ter mais informações, consulte Restrições de tamanho e configuração de um volume do EBS.
6. (`io1`, `io2` e `gp3` apenas) Em IOPS, insira o número máximo de operações de entrada/saída por segundo (IOPS) que o volume deve oferecer.
7. (`gp3` apenas) Em Throughput, insira a throughput que o volume deve fornecer, em MiB/s.
8. Para Zona de disponibilidade, escolha a zona de disponibilidade na qual criar o volume. Um volume só pode ser anexado a uma instância que esteja na mesma zona de disponibilidade.
9. Em Snapshot ID (ID do snapshot), mantenha o valor padrão (não crie volume a partir de um snapshot).

10. (`io1` e `io2` apenas) Para habilitar o volume para vinculação múltipla do Amazon EBS, selecione Enable Multi-Attach (Habilitar vinculação múltipla). Para ter mais informações, consulte Anexar um volume a várias instâncias com o Multi-Attach do Amazon EBS.
11. Defina o status de criptografia do volume.

    Se sua conta for habilitada para criptografia por padrão, a criptografia será habilitada automaticamente e você não poderá desabilitá-la. É possível escolher a chave do KMS a ser usada para criptografar o volume.

    Se sua conta não for habilitada para criptografia por padrão, a criptografia será opcional. Para criptografar o volume, para Encyption (Criptografia), escolha Encrypt this volume (Criptografar este volume) e selecione a chave do KMS a ser usada.

    > **Note**
    >
    > Os volumes criptografados só podem ser anexados a instâncias que suportem a criptografia do Amazon EBS. Para ter mais informações, consulte Criptografia do Amazon EBS.

12. (Opcional) Para atribuir tags personalizadas ao volume, na seção Tags, escolha Adicionar tag e insira um par de chave e valor de tag.
13. Escolha Create volume (Criar volume).

    > **Note**
    >
    > O volume está pronto para uso quando o Volume state (Estado do volume) é available (disponível).

14. Para usar o volume, anexe-o a uma instância. Para ter mais informações, consulte Vincular um volume de Amazon EBS a uma instância.

AWS CLI

Para criar um volume vazio do EBS usando o AWS CLI

Use o comando create-volume.

O volume está pronto para uso quando o `state` é `available`.

Tools for Windows PowerShell

Para criar um volume vazio do EBS usando as Ferramentas para Windows PowerShell

Use o comando New-EC2Volume.

O volume está pronto para uso quando o `state` é `available`.

Criar um volume a partir de um snapshot

Os volumes criados de snapshots são carregados lentamente em segundo plano. Isso significa que não há necessidade de esperar que todos os dados sejam transferidos do Amazon S3 para o volume do EBS para que a instância possa começar a acessar um volume anexado e todos os seus dados. Se sua instância acessar dados que ainda não foram carregados, o volume imediatamente baixará os dados solicitados do Amazon S3 e continuará carregando o restante dos dados do volume em segundo plano. A performance do volume é obtida depois que todos os blocos forem obtidos por download e gravados no volume. Para evitar a ocorrência de performance inicial em um ambiente de produção, consulte Inicializar volumes de Amazon EBS.

Os novos volumes do EBS criados de snapshots criptografados são criptografados automaticamente. Você também pode criptografar um volume on-the-fly enquanto o restaura a partir de um snapshot não criptografado. Os volumes criptografados só podem ser anexados a tipos de instâncias que oferecem suporte à criptografia do EBS. Para ter mais informações, consulte Tipos de instâncias compatíveis.

Você pode criar um volume a partir de um snapshot usando um dos métodos a seguir.

Console

Para restaurar um volume do EBS a partir de um snapshot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Escolha Create volume (Criar volume).
4. Em Volume type (Tipo de volume), escolha o tipo de volume a ser criado. Para ter mais informações, consulte Tipos de volume do Amazon EBS.

   O SSD `gp3` de uso geral é a seleção padrão.

5. Para Size (Tamanho), informe o tamanho do volume, em GiB. Para ter mais informações, consulte Restrições de tamanho e configuração de um volume do EBS.
6. (`io1`, `io2` e `gp3` apenas) Em IOPS, insira o número máximo de operações de entrada/saída por segundo (IOPS) que o volume deve oferecer.
7. (`gp3` apenas) Em Throughput, insira a throughput que o volume deve fornecer, em MiB/s.
8. Para Zona de disponibilidade, escolha a zona de disponibilidade na qual criar o volume. Um volume só pode ser anexado a instâncias que estejam na mesma zona de disponibilidade.
9. Em Snapshot ID (ID do snapshot) selecione o snapshot a partir do qual o volume será criado.
10. Defina o status de criptografia do volume.

    Se o snapshot selecionado for criptografado ou se sua conta for habilitada para criptografia, por padrão, a criptografia será habilitada automaticamente e você não poderá desabilitá-la. É possível escolher a chave do KMS a ser usada para criptografar o volume.

    Se o snapshot selecionado não for criptografado e sua conta, por padrão, não for habilitada para criptografia, a criptografia será opcional. Para criptografar o volume, em Encyption (Criptografia), escolha Encrypt this volume (Criptografar este volume) e selecione a chave do KMS a ser usada.

    > **Note**
    >
    > Os volumes criptografados só podem ser anexados a instâncias que suportem a criptografia do Amazon EBS. Para ter mais informações, consulte Criptografia do Amazon EBS.

11. (Opcional) Para atribuir tags personalizadas ao volume, na seção Tags, escolha Adicionar tag e insira um par de chave e valor de tag.
12. Escolha Criar volume.

    > **Note**
    >
    > O volume está pronto para uso quando o Volume state (Estado do volume) é available (disponível).

13. Para usar o volume, anexe-o a uma instância. Para ter mais informações, consulte Vincular um volume de Amazon EBS a uma instância.

AWS CLI

Para criar um volume do EBS a partir de um snapshot usando o AWS CLI

Use o comando create-volume.

O volume está pronto para uso quando o `state` é `available`.

Tools for Windows PowerShell

Para criar um volume do EBS a partir de um snapshot usando as Ferramentas para Windows PowerShell

Use o comando New-EC2Volume.

O volume está pronto para uso quando o `state` é `available`.

Vincular um volume de Amazon EBS a uma instância

É possível anexar um volume do EBS disponível a uma ou mais de suas instâncias que estejam na mesma zona de disponibilidade que o volume.

Para obter informações sobre como adicionar volumes do EBS à instância no início da execução, consulte mapeamento de dispositivos de blocos da instância.

Considerações

- Determine quantos volumes você pode associar à sua instância. O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Para obter mais informações, consulte Limites de volume por instância.
- Determine se é possível anexar seu volume a várias instâncias e habilite a opção Anexar várias. Para ter mais informações, consulte Anexar um volume a várias instâncias com o Multi-Attach do Amazon EBS.
- Se um volume for criptografado, ele só poderá ser associado a uma instância que suporte a criptografia do Amazon EBS. Para ter mais informações, consulte Tipos de instâncias compatíveis.
- Se um volume tiver um código de AWS Marketplace produto:
  - Só é possível anexar um volume a uma instância interrompida.
  - Você deve estar inscrito no AWS Marketplace código que está no volume.

- A configuração da instância, como seu tipo e sistema operacional, deve oferecer suporte a esse AWS Marketplace código específico. Por exemplo, você não pode obter um volume de uma instância do Windows e associá-la a uma instância do Linux.
- AWS Marketplace os códigos do produto são copiados do volume para a instância.

É possível anexar um volume a uma instância usando um dos métodos a seguir.

Console

Para associar um volume do EBS a uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione um volume a ser anexado e escolha Actions (Ações) e Attach Volume (Anexar volume).

   > **Note**
   >
   > Você só pode anexar volumes que estejam no estado `Available`.

4. Em Instance (Instância), insira o ID da instância ou selecione a instância na lista de opções.

   > **Note**
   >
   > - O volume deve ser anexado a uma instância na mesma zona de disponibilidade.
   > - Se o volume for criptografado, ele só poderá ser anexado a uma instância que suporte a criptografia do Amazon EBS. Para ter mais informações, consulte Criptografia do Amazon EBS.

5. Em Nome do dispositivo, faça o seguinte:

   - Para um volume raiz, selecione o nome do dispositivo necessário na seção Reservado para volume raiz da lista. Normalmente `/dev/sda1` ou `/dev/xvda` para instâncias Linux, dependendo da AMI, ou `/dev/sda1` para instâncias do Windows.
   - Para volumes de dados, selecione um nome de dispositivo disponível na seção Recomendado para volumes de dados da lista.

- Para usar um nome de dispositivo personalizado, selecione Especificar um nome de dispositivo personalizado e, em seguida, insira o nome do dispositivo a ser usado.

  Esse nome de dispositivo é usado pelo Amazon EC2. O driver de dispositivo de blocos da instância pode atribuir um nome de volume diferente ao montar o volume. Para obter mais informações, consulte nomes de dispositivos em instâncias Linux ou nomes de dispositivos em instâncias do Windows.

6. Selecione Attach volume (Anexar volume).
7. Conecte à instância e monte o volume. Para ter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso.

AWS CLI

Para anexar um volume do EBS a uma instância usando o AWS CLI

Use o comando attach-volume.

Tools for Windows PowerShell

Para anexar um volume do EBS a uma instância usando as Ferramentas para Windows PowerShell

Use o comando Add-EC2Volume.

> **Note**
>
> - Se você tentar anexar vários volumes que façam com que o limite de volume do tipo de instância seja excedido, a solicitação falhará. Para obter mais informações, consulte Limites de volume por instância.
> - Em algumas situações, é possível descobrir que um volume além do volume associado a `/dev/xvda` ou `/dev/sda` tornou-se o volume do dispositivo raiz da sua instância. Isso pode acontecer quando você associar o volume do dispositivo raiz de outra instância, ou um volume criado a partir do snapshot de um volume do dispositivo raiz, a uma instância com um volume do dispositivo raiz existente. Para obter mais informações, consulte Inicialização a partir do volume errado.

Anexar um volume a várias instâncias com o Multi-Attach do Amazon EBS

O Amazon EBS Multi-Attach permite que você anexe um único volume SSD de IOPS provisionadas (`io1` ou `io2`) a várias instâncias na mesma zona de disponibilidade. É possível anexar vários volumes habilitados para Multi-Attach a uma instância ou conjunto de instâncias. Cada instância à qual o volume está anexado tem permissão completa de leitura e gravação no volume compartilhado. O Multi-Attach facilita obter maior disponibilidade da aplicação em aplicações que gerenciam operações de gravação simultâneas.

Conteúdo

Considerações e limitações

- Os volumes habilitados para Multi-Attach podem ser anexados a até 16 instâncias criadas no Nitro System que estejam na mesma zona de disponibilidade.
- As instâncias Linux são compatíveis com volumes `io1` e `io2` habilitados para Multi-Attach. As instâncias Windows são compatíveis somente com volumes `io2` habilitados para Multi-Attach.
- O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Para obter mais informações, consulte Limites de volume por instância.
- O Multi-Attach é compatível exclusivamente com volumes SSD de IOPS provisionadas (`io1` e `io2`.
- A anexação múltipla de volumes `io1` está disponível somente nas seguintes regiões: Leste dos EUA (N. da Virgínia), Oeste dos EUA (Oregon) e Ásia-Pacífico (Seul).

  O Multi-Attach para `io2` está disponível em todas as regiões compatíveis com `io2`.

> **Note**
>
> Para melhorar a performance, a consistência e a durabilidade a um custo menor, recomendamos que você use volumes `io2`.

- Os volumes `io1` com o Multi-Attach habilitado não são compatíveis com instâncias criadas no Nitro System que só são compatíveis com o protocolo de rede Scalable Reliable Datagram (SRD). Para usar o Multi-Attach com esses tipos de instância, você deve usar volumes `io2` Block Express.
- Os sistemas de arquivos padrão, como XFS e EXT4, não foram projetados para serem acessados simultaneamente por vários servidores, como as instâncias do EC2. Você deve usar um sistema de arquivos clusterizado para garantir a resiliência e a confiabilidade dos dados para suas cargas de trabalho de produção.
- Os volumes `io2` ativados para Multi-Attach não suportam isolamento de E/S. Os protocolos de cercas de E/S controlam o acesso de gravação em um ambiente de armazenamento compartilhado para manter a consistência dos dados. Suas aplicações devem fornecer uma ordem de gravação para as instâncias anexadas para manter a consistência dos dados. Para ter mais informações, consulte Reservas NVMe.

  Os volumes `io1` ativados para Multi-Attach não suportam isolamento de E/S.
- Volumes habilitados para Multi-Attach não podem ser criados como volumes de inicialização.
- Os volumes habilitados para Multi-Attach podem ser anexados a um mapeamento de dispositivo de bloco por instância.
- O Multi-Attach não pode ser habilitado durante a execução da instância usando o console RunInstances ou a API do Amazon EC2.
- Os volumes habilitados para Multi-Attach que têm um problema na camada da infraestrutura do Amazon EBS não estão disponíveis para todas as instâncias anexadas. Problemas no Amazon EC2 ou na camada de rede podem afetar apenas algumas instâncias anexadas.
- A tabela a seguir mostra o suporte a modificação de volumes para volumes `io1` e `io2` habilitados para Multi-Attach.

	Volumes do **io2**	Volumes do **io1**
Modificar tipo de volume	✗	✗
Modificar tamanho do volume	✓	✗
Modificar as IOPS provisionadas	✓	✗
Ativar Multi-Attach	✓ *	✗
Desativar Multi-Attach	✓ *	✗

* Você não pode ativar ou desativar o Multi-Attach enquanto o volume estiver associado a uma instância.

Performance

Cada instância anexada pode direcionar sua performance máxima de IOPS até a performance máxima provisionada do volume. No entanto, a performance agregada de todas as instâncias anexadas não pode exceder a performance máxima provisionada do volume. Se a demanda das instâncias anexadas por IOPS for maior que as IOPS provisionadas do volume, o volume não excederá sua performance provisionada.

Por exemplo, digamos que você crie um volume `io2` habilitado para Multi-Attach com `80,000` IOPS provisionados e anexe-o a uma instância `m7g.large` que suporta até `40,000` IOPS e um `r7g.12xlarge` instância que suporta até `60,000` IOPS. Cada instância pode direcionar seu máximo de IOPS, pois ele é menor do que as IOPS do volume de `80,000`. No entanto, se as duas instâncias direcionarem a E/S para o volume simultaneamente, suas IOPS combinadas não poderão exceder a performance provisionada do volume de `80,000` IOPS.

Para obter uma performance consistente, é uma prática recomendada equilibrar a E/S direcionada de instâncias anexadas entre os setores de um volume habilitado para Multi-Attach.

Como trabalhar com Multi-Attach

Os volumes habilitados para Multi-Attach podem ser gerenciados da mesma maneira como você gerenciaria qualquer outro volume do Amazon EBS. No entanto, para usar a funcionalidade Multi-Attach, é necessário habilitá-la para o volume. Quando um volume é criado, o Multi-Attach está desabilitado por padrão.

Sumário

Ativar Multi-Attach

Você pode ativar o Multi-Attach durante a criação do volume. Use um dos métodos a seguir.

Console

Como habilitar o Multi-Attach durante a criação do volume

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Escolha Create volume (Criar volume).
4. Em Tipo de volume, escolha SSD de IOPS provisionadas (**io1**) ou SSD de IOPS provisionadas (**io2**).
5. Em Size (Tamanho) e IOPS, escolha o tamanho necessário do volume e o número de IOPS a serem provisionadas.
6. Em Availability Zone (Zona de disponibilidade), escolha a mesma Zona de disponibilidade em que as instâncias se encontram.
7. Em Amazon EBS Multi-Attach (Vinculação múltipla do Amazon EBS), escolha Enable Multi-Attach (Habilitar vinculação múltipla).

8. (Opcional) Em Snapshot ID (ID do snapshot), escolha o snapshot a partir do qual o volume será criado.
9. Defina o status de criptografia do volume.

   Se o snapshot selecionado for criptografado ou se sua conta for habilitada para criptografia, por padrão, a criptografia será habilitada automaticamente e você não poderá desabilitá-la. É possível escolher a chave do KMS a ser usada para criptografar o volume.

   Se o snapshot selecionado não for criptografado e sua conta, por padrão, não for habilitada para criptografia, a criptografia será opcional. Para criptografar o volume, em Encyption (Criptografia), escolha Encrypt this volume (Criptografar este volume) e selecione a chave do KMS a ser usada.

   > **Note**
   >
   > Volumes criptografados só podem ser anexados a instâncias que ofereçam suporte à criptografia do Amazon EBS. Para ter mais informações, consulte Criptografia do Amazon EBS.

10. (Opcional) Para atribuir tags personalizadas ao volume, na seção Tags, escolha Adicionar tag e insira um par de chave e valor de tag.
11. Escolha Create volume (Criar volume).

Command line

Como habilitar o Multi-Attach durante a criação do volume

Use o comando create-volume e especifique o parâmetro `--multi-attach-enabled`.

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

Você também pode ativar Multi-Attach para volumes `io2` após a criação, mas somente se eles não estiverem anexados a nenhuma instância.

> **Note**
>
> Você não pode habilitar o Multi-Attach para volumes de `io1` após a criação.

Use um dos métodos a seguir para ativar o Multi-Attach para um volume `io2` após a criação.

Console

Para ativar o Multi-Attach após a criação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume e escolha Actions (Ações), Modify Volume (Modificar volume).
4. Em Amazon EBS Multi-Attach (Vinculação múltipla do Amazon EBS), escolha Enable Multi-Attach (Habilitar vinculação múltipla).
5. Selecione Modify.

Command line

Para ativar o Multi-Attach após a criação

Use o comando modify-volume e especifique o parâmetro `--multi-attach-enabled`.

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

Desativar Multi-Attach

É possível desativar o Multi-Attach para um volume de `io2` somente se ele estiver conectado a não mais do que uma instância.

> **Note**
>
> Não é possível desativar o Multi-Attach para volumes de `io1` após a criação.

Use um dos seguintes métodos para desativar o Multi-Attach para um volume de `io2`.

Console

Para desativar o Multi-Attach após a criação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume e escolha Actions (Ações), Modify Volume (Modificar volume).
4. Em Amazon EBS Multi-Attach (Vinculação múltipla do Amazon EBS), limpe Enable Multi-Attach (Habilitar vinculação múltipla).
5. Selecione Modify.

Command line

Para desativar o Multi-Attach após a criação

Use o comando modify-volume e especifique o parâmetro `-no-multi-attach-enabled`.

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

Anexar um volume a instâncias

Você anexa um volume habilitado para vinculação múltipla a uma instância da mesma maneira como anexa qualquer outro volume do EBS. Para obter mais informações, consulte Vincular um volume de Amazon EBS a uma instância.

Excluir no encerramento

Os volumes habilitados para Multi-Attach serão excluídos no encerramento da instância se a última instância anexada for encerrada, e se essa instância estiver configurada para excluir o volume ao encerrar. Se o volume estiver anexado a várias instâncias que têm configurações diferentes de exclusão no encerramento em seus mapeamentos de dispositivos de blocos de volume, a configuração de mapeamento de dispositivo de blocos da última instância anexada determinará o comportamento da exclusão no encerramento.

Para garantir a exclusão previsível no comportamento de encerramento, habilite ou desabilite a exclusão no encerramento para todas as instâncias às quais o volume está anexado.

Por padrão, quando um volume é anexado a uma instância, a configuração de exclusão no encerramento do mapeamento de dispositivo de blocos é definida como falsa. Para habilitar a exclusão no encerramento para um volume habilitado para Multi-Attach, modifique o mapeamento de dispositivo de blocos.

Se desejar que o volume seja excluído quando as instâncias anexadas forem encerradas, habilite a exclusão no encerramento no mapeamento de dispositivo de blocos para todas as instâncias anexadas. Para reter o volume depois que as instâncias anexadas tiverem sido encerradas, desabilite a exclusão no encerramento no mapeamento de dispositivo de blocos para todas as instâncias anexadas. Para obter mais informações, consulte Preservar dados quando uma instância for encerrada.

É possível modificar a configuração de exclusão no encerramento de uma instância na execução ou depois que ela for executada. Se você habilitar ou desabilitar a exclusão no encerramento durante a execução da instância, as configurações se aplicarão somente aos volumes anexados na execução. Se você anexar um volume a uma instância após a execução, deverá definir explicitamente o comportamento de exclusão no encerramento para esse volume.

É possível modificar a configuração de exclusão no encerramento de uma instância usando somente as ferramentas da linha de comando.

Como modificar a configuração de exclusão no encerramento de uma instância existente

Use o comando modify-instance-attribute e especifique o atributo `DeleteOnTermination` em `--block-device-mappings option`.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-
mappings file://mapping.json
```

Especifique o seguinte em `mapping.json`.

```
[
  {
    "DeviceName": "/dev/sdf",
    "Ebs": {
      "DeleteOnTermination": true|false
    }
  }
]
```

Monitorar um volume habilitado para Multi-Attach

Você pode monitorar um volume habilitado para Multi-Attach usando as CloudWatch métricas dos volumes do Amazon EBS. Para ter mais informações, consulte CloudWatch Métricas da Amazon para Amazon EBS.

Os dados são agregados em todas as instâncias anexadas. Você não pode monitorar métricas para instâncias anexadas individuais.

Definição de preço e faturamento

Não há cobranças adicionais pelo uso do recurso Multi-Attach do Amazon EBS Você receberá as cobranças padrão aplicáveis aos volumes SSD de IOPS provisionadas (`io1` e `io2`). Para obter mais informações, consulte Definição de preço do Amazon EBS.

Reservas NVMe

`io2`Os volumes habilitados para Multi-Attach oferecem suporte às reservas NVMe, que é um conjunto de protocolos de vedação de armazenamento padrão do setor. Esses protocolos permitem criar e gerenciar reservas que controlam e coordenam o acesso de várias instâncias a um volume compartilhado. As reservas são usadas por aplicativos de armazenamento compartilhado para garantir a consistência dos dados.

Tópicos

Requisitos

As reservas NVMe são compatíveis somente com volumes compatíveis com Multi-Attach. `io2` Os volumes habilitados para Multi-Attach só podem ser anexados a instâncias criadas no sistema Nitro.

As reservas NVMe são compatíveis com os seguintes sistemas operacionais:

- SUSE Linux Enterprise 12 SP3 e posterior
- RHEL 8.3 e versões posteriores

- Amazon Linux 2 e posterior
- Windows Server 2016 e posterior

> **Note**
>
> Para AMIs do Windows Server compatíveis datadas de 2023.09.13 e posteriores, os drivers NVMe necessários estão incluídos. Para AMIs anteriores, você deve atualizar para a versão 1.5.0 ou posterior do driver NVMe. Para obter mais informações, consulte Drivers do AWS NVMe para instâncias Windows.

Se você estiver usando o EC2Launch v2 para inicializar seus discos, você deve atualizar para a versão 2.0.1521 ou posterior. Para obter mais informações, consulte Configurar instâncias do Windows usando o EC2Launch v2.

Habilitando o suporte para reservas de NVMe

O suporte para reservas NVMe está ativado por padrão para todos os `io2` volumes habilitados para Multi-Attach criados após 18 de setembro de 2023.

Para habilitar o suporte para reservas de NVMe para `io2` volumes existentes criados antes de 18 de setembro de 2023, você deve separar todas as instâncias do volume e, em seguida, reconectar as instâncias necessárias. Todos os anexos feitos após a separação de todas as instâncias terão as reservas de NVMe ativadas.

Comandos de reserva NVMe compatíveis

O Amazon EBS oferece suporte aos seguintes comandos de reserva do NVMe:

Registro de reservas

Registra, cancela o registro ou substitui uma chave de reserva. Uma chave de registro é usada para identificar e autenticar uma instância. O registro de uma chave de reserva com um volume cria uma associação entre a instância e o volume. Você deve registrar a instância com o volume antes que a instância possa adquirir uma reserva.

Reserva > Adquirir

Adquire uma reserva em um volume, antecipa uma reserva mantida em um namespace e aborta uma reserva mantida em um volume. Os seguintes tipos de reserva podem ser adquiridos:

- Escreva uma reserva exclusiva
- Reserva de acesso exclusivo
- Escreva com exclusividade - Reserva exclusiva para inscritos
- Acesso exclusivo - Reserva somente para inscritos
- Escreva com exclusividade - Reserva para todos os inscritos
- Acesso exclusivo - Reserva para todos os inscritos

Liberação de reserva

Libera ou limpa uma reserva mantida em um volume.

Relatório de reserva

Descreve o status de registro e reserva de um volume.

Definição de preço

Não há custos adicionais para ativar e usar o Multi-Attach.

Disponibilizar um volume do Amazon EBS para uso

Depois de anexar um volume do Amazon EBS à instância, ele é exposto como um dispositivo de blocos. É possível formatar o volume com qualquer sistema de arquivos e então montá-lo. Após disponibilizar o volume do EBS para uso, será possível acessá-lo das mesmas maneiras que acessa qualquer outro volume. Todos os dados gravados nesse sistema de arquivos são gravados no volume do EBS e são transparentes para aplicações que usam o dispositivo.

É possível tirar snapshots do volume do EBS para fins de backup ou para usar como linha de base quando criar outro volume. Para ter mais informações, consulte Snapshots do Amazon EBS.

Se o volume do EBS que estiver preparando para uso for maior que 2 TiB, você deverá usar um esquema de particionamento GPT para acessar todo o volume. Para ter mais informações, consulte Restrições de tamanho e configuração de um volume do EBS.

Instâncias do Linux

Formatar e montar um volume anexado

Suponha que você tenha uma instância do EC2 com um volume do EBS para o dispositivo raiz, `/dev/xvda`, e que tenha anexado um volume do EBS vazio à instância usando o `/dev/sdf`. Use o procedimento a seguir para disponibilizar o volume recém-anexado para uso.

Para formatar e montar um volume do EBS no Linux

1. Conecte-se à sua instância usando SSH. Para obter mais informações, consulte Conectar-se à instância do Linux.
2. O dispositivo pode ser anexado à instância com um nome de dispositivo diferente do especificado no mapeamento de dispositivos de blocos. Para obter mais informações, consulte Nomes de dispositivos em instâncias do Linux. Use o comando lsblk para visualizar os dispositivos de disco disponíveis e seus pontos de montagem (se aplicável) para ajudá-lo a determinar o nome de dispositivo correto a usar. A saída de lsblk remove o prefixo `/dev/` dos caminhos completos do dispositivo.

   Veja a seguir um exemplo de saída para uma instância criada no Nitro System que expõe os volumes do EBS como dispositivos de blocos do NVMe. O dispositivo raiz é `/dev/nvme0n1`, que tem duas partições chamadas `nvme0n1p1` e `nvme0n1p128`. O volume anexado é `/dev/nvme1n1`, que ainda não tem partições e não está montado.

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

   Este é um exemplo de saída de uma instância T2. O dispositivo raiz é `/dev/xvda`, que tem uma partição chamada `xvda1`. O volume anexado é `/dev/xvdf`, que ainda não tem partições e não está montado.

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   -xvda1  202:1    0    8G  0 part /
   xvdf    202:80   0   10G  0 disk
   ```
3. Determine se existe um sistema de arquivos no volume. Os novos volumes são dispositivos de blocos raw, e crie um sistema de arquivos neles antes que possa montá-los e usá-los. Os volumes que foram criados de snapshots provavelmente já têm um sistema de arquivos neles. Se você criar um sistema de arquivos sobre o sistema de arquivos existente, a operação sobrescreverá seus dados.

Use um ou ambos os métodos a seguir para determinar se há um sistema de arquivos no volume:

- Use o comando file -s para obter informações sobre o dispositivo específico, como o tipo de sistema de arquivos. Se a saída mostrar simplesmente `data`, como no exemplo de saída a seguir, não há sistema de arquivos no dispositivo

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

  Se o dispositivo tiver um sistema de arquivos, o comando mostrará informações sobre o tipo de sistema de arquivos. Por exemplo, a saída a seguir mostra um dispositivo raiz com o sistema de arquivos XFS.

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

- Use o comando lsblk -f para obter informações sobre todos os dispositivos vinculados à instância.

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

  Por exemplo, a saída a seguir mostra que existem três dispositivos vinculados às instâncias —`nvme1n1nvme2n1` e `nvme0n1`. A primeira coluna lista os dispositivos e suas partições. A coluna `FSTYPE` exibe o tipo de sistema de arquivos para cada dispositivo. Se a coluna estiver vazia para um dispositivo específico, isso significa que o dispositivo não possui um sistema de arquivos. Neste caso, o dispositivo `nvme1n1` e as partições `nvme0n1p1` no dispositivo `nvme0n1` são formatados usando o sistema de arquivos XFS, enquanto o dispositivo `nvme2n1` e as partições `nvme0n1p128` no dispositivo `nvme0n1` não têm sistemas de arquivos.

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

Se a saída destes comandos mostrar que não há nenhum sistema de arquivos no dispositivo, você deverá criar um.

4. (Condicional) Se você descobriu que há um sistema de arquivos no dispositivo na etapa anterior, ignore esta etapa. Se você tiver um volume vazio, use o comando mkfs -t para criar um sistema de arquivos no volume.

> **Warning**
>
> Não use esse comando se você estiver montando um volume que já contenha dados (por exemplo, um volume que foi criado de um snapshot). Caso contrário, você formatará o volume e excluirá os dados existentes.

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

Se você receber um erro de que `mkfs.xfs` não foi encontrado, use o seguinte comando para instalar as ferramentas do XFS e repita o comando anterior:

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

5. Use o comando mkdir para criar um diretório de ponto de montagem para o volume. O ponto de montagem é o local onde o volume está localizado na árvore do sistema de arquivos e onde você lê e grava arquivos depois de montar o volume. O exemplo a seguir cria um diretório denominado `/data`.

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

6. Monte o volume ou a partição no diretório de ponto de montagem criado na etapa anterior.

   Se o volume não tiver partições, use o comando a seguir e especifique o nome do dispositivo para montar o volume inteiro.

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

   Se o volume tiver partições, use o comando a seguir e especifique o nome da partição para montar uma partição.

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

7. Revise as permissões de arquivo da montagem do seu novo volume para assegurar-se de que os usuários e aplicações podem gravar no volume. Para mais informações sobre as permissões de arquivos, consulte Segurança de arquivos no Projeto de documentação do Linux.
8. O ponto de montagem não é preservado automaticamente após a reinicialização da instância. Para montar automaticamente esse volume do EBS após a reinicialização, consulte Montar automaticamente um volume anexado após a reinicialização.

Montar automaticamente um volume anexado após a reinicialização

Para montar um volume anexado do EBS em cada reinicialização do sistema, adicione uma entrada para o dispositivo ao arquivo `/etc/fstab`.

É possível usar o nome do dispositivo, como `/dev/xvdf`, no `/etc/fstab`, mas recomendamos o uso do identificador universal exclusivo (UUID) de 128 bits do dispositivo. Os nomes dos dispositivos podem mudar, mas o UUID persiste durante todo o ciclo de vida da partição. Usando o UUID, você reduz as possibilidades de o sistema se tornar não inicializável após uma reconfiguração de hardware. Para obter mais informações, consulte Identificar o dispositivo EBS.

Para montar um volume anexado automaticamente após a reinicialização

1. (Opcional) Crie um backup do seu arquivo `/etc/fstab` para usar se você destruir ou excluir acidentalmente esse arquivo quando for editá-lo.

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

2. Use o comando blkid para encontrar o UUID do dispositivo. Anote o UUID do dispositivo que você deseja montar após a reinicialização. Você vai precisar dele na etapa seguinte.

   Por exemplo, o comando a seguir mostra que existem dois dispositivos montados na instância e mostra os UUIDs para ambos os dispositivos.

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

Para Ubuntu 18.04, use o comando lsblk.

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

3. Abra o arquivo `/etc/fstab` usando qualquer editor de texto (como nano ou vim).

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

4. Adicione a entrada a seguir ao `/etc/fstab` para montar o dispositivo no ponto de montagem especificado. Os campos são o valor de UUID retornado pelo blkid (ou lsblk, para Ubuntu 18.04), ponto de montagem, sistema de arquivos e opções recomendadas de montagem do sistema de arquivos. Para obter mais informações sobre os campos obrigatórios, execute `man fstab` para abrir o fstab manual.

   No exemplo a seguir, montamos o dispositivo com UUID `aebf131c-6957-451e-8d34-ec978d9581ae` no ponto de montagem `/data` e usamos o sistema de arquivos `xfs`. Também usamos as flags `nofail` e `defaults`. Especificamos `0` para evitar que o sistema de arquivos seja despejado, e especificamos 2 para indicar que ele é um dispositivo não raiz.

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

> **Note**
>
> Se você inicializar a instância sem esse volume anexado (por exemplo, depois de mover o volume para outra instância), a opção de montagem `nofail` permitirá que a instância seja inicializada mesmo se houver erros na montagem do volume. Os derivados de Debian, incluindo versões de Ubuntu anteriores à 16.04, também devem adicionar a opção de montagem `nobootwait`.

5. Para verificar se sua entrada funciona, execute os seguintes comandos para desmontar o dispositivo e, depois, montar todos os sistemas de arquivos em `/etc/fstab`. Se não houver erros, o arquivo `/etc/fstab` será válido e o sistema de arquivos será montado automaticamente após ser reinicializado.

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

Se você receber uma mensagem de erro, resolva os erros no arquivo.

> **Warning**
>
> Erros no arquivo `/etc/fstab` podem impedir a inicialização de um sistema. Não encerre um sistema que tenha erros no arquivo `/etc/fstab`.

Se você não souber corrigir os erros no `/etc/fstab` e criou um arquivo de backup na primeira etapa desse procedimento, poderá restaurar a partir do arquivo de backup usando o comando a seguir.

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

Instâncias do Windows

Use um dos métodos a seguir para disponibilizar um volume em uma instância do Windows.

PowerShell

Para disponibilizar todos os volumes do EBS com partições brutas para uso com o Windows PowerShell

1. Faça login na instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte Conectar-se à sua instância do Windows.
2. Na barra de tarefas, abra o menu Iniciar e escolha Windows. PowerShell
3. Use a série fornecida de PowerShell comandos do Windows no PowerShell prompt aberto. O script executa as seguintes ações por padrão:
    1. Interrompe o serviço ShellHWDetection.
    2. Enumera discos em que o estilo de partição é bruto.
    3. Cria uma nova partição que abrange o tamanho máximo que o disco e o tipo de partição suportarão.
    4. Atribui uma letra de unidade disponível.
    5. Formata o sistema de arquivos como NTFS com o rótulo do sistema de arquivos especificado.

6. Inicia o serviço ShellHWDetection novamente.

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

DiskPart command line tool

Para disponibilizar um volume do EBS para uso com a ferramenta de linha de DiskPart comando

1. Faça login na instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte Conectar-se à sua instância do Windows.
2. Determine o número do disco que você deseja disponibilizar:
   1. Abra o menu Iniciar e selecione Windows PowerShell.
   2. Use o Cmdlet `Get-Disk` para recuperar uma lista de discos disponíveis.
   3. Na saída do comando, observe o número correspondente ao disco que você está disponibilizando.
3. Crie um arquivo de script para executar DiskPart comandos:
   1. Abra o menu Start (Iniciar) e selecione o File explorer (Gerenciador de arquivos).
   2. Navegue até um diretório, como C:\, para armazenar o arquivo de script.
   3. Escolha ou clique com o botão direito do mouse em um espaço vazio na pasta para abrir a caixa de diálogo, posicionar o cursor sobre New (Novo) para acessar o menu de contexto e, depois, escolha Text document (Documento de texto).
   4. Nomeie o arquivo de texto como `diskpart.txt`.
4. Adicione os comandos a seguir ao arquivo de script. Talvez seja necessário modificar o número do disco, o tipo de partição, o rótulo do volume e a letra da unidade. O script executa as seguintes ações por padrão:
   1. Seleciona o disco 1 para modificação.
   2. Configura o volume para usar a estrutura de partição do registro mestre de inicialização (MBR).

3. Formata o volume como um volume NTFS.
4. Define o rótulo de volume.
5. Atribui ao volume uma letra de unidade.

> **Warning**
>
> Se você estiver montando um volume que já tenha dados, não reformate o volume. Caso contrário, excluirá os dados existentes.

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

Para obter mais informações, consulte DiskPart Sintaxe e parâmetros.

5. Abra um prompt de comando, navegue até a pasta na qual o script está localizado e execute o seguinte comando para tornar um volume disponível para uso no disco especificado:

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

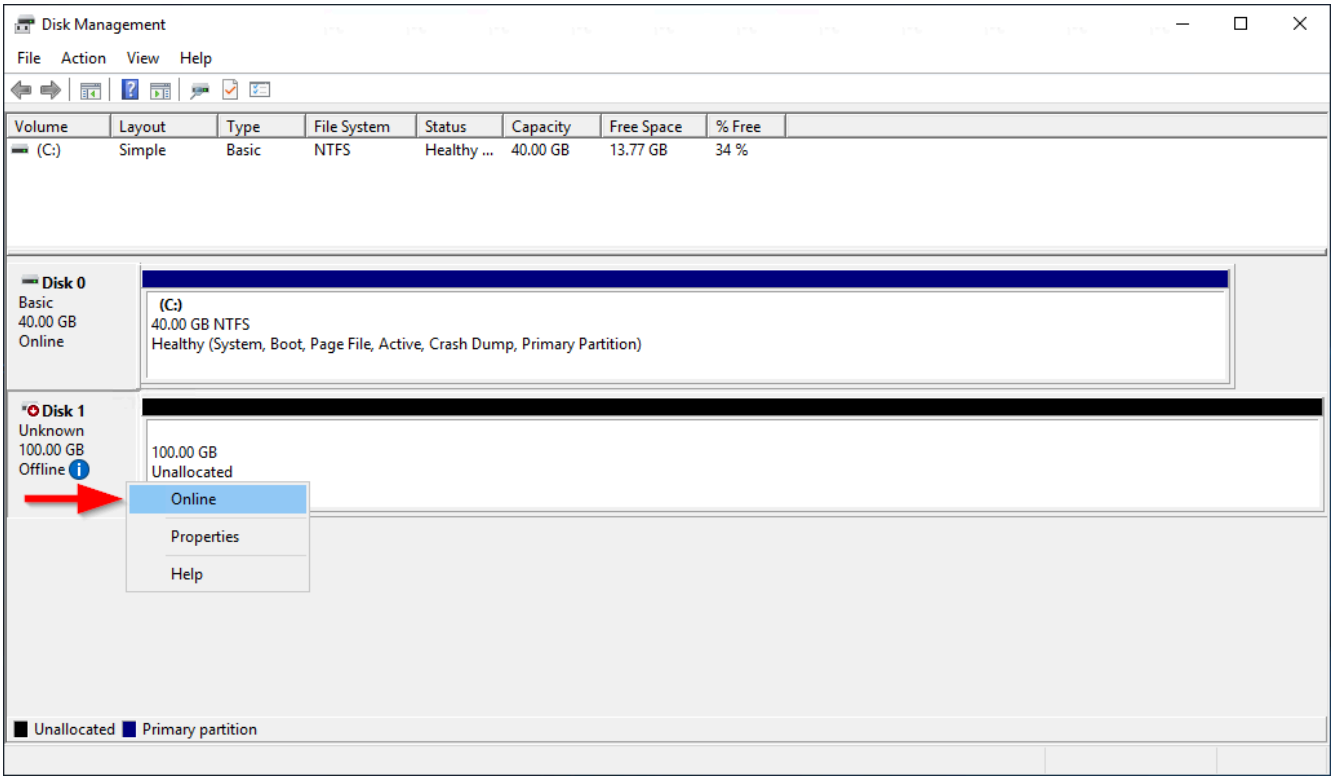
Disk Management utility

Para disponibilizar um volume do EBS para uso por meio do utilitário de gerenciamento de disco

1. Faça login na instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte Conectar-se à sua instância do Windows.
2. Inicie o utilitário de Gerenciamento de Disco. Na barra de ferramentas, abra o menu de contexto (clique com o botão direito do mouse) no logo do Windows e escolha Disk Management (Gerenciamento de disco).

> **Note**
>
> No Windows Server 2008, escolha Start (Iniciar), Administrative Tools (Ferramentas administrativas), Computer Management (Gerenciamento do computador), Disk Management (Gerenciamento de disco).

3. Traga o volume online. No painel inferior, abra o menu de contexto (clique com o botão direito do mouse) no painel esquerdo para o disco do volume do EBS. Escolha Online.

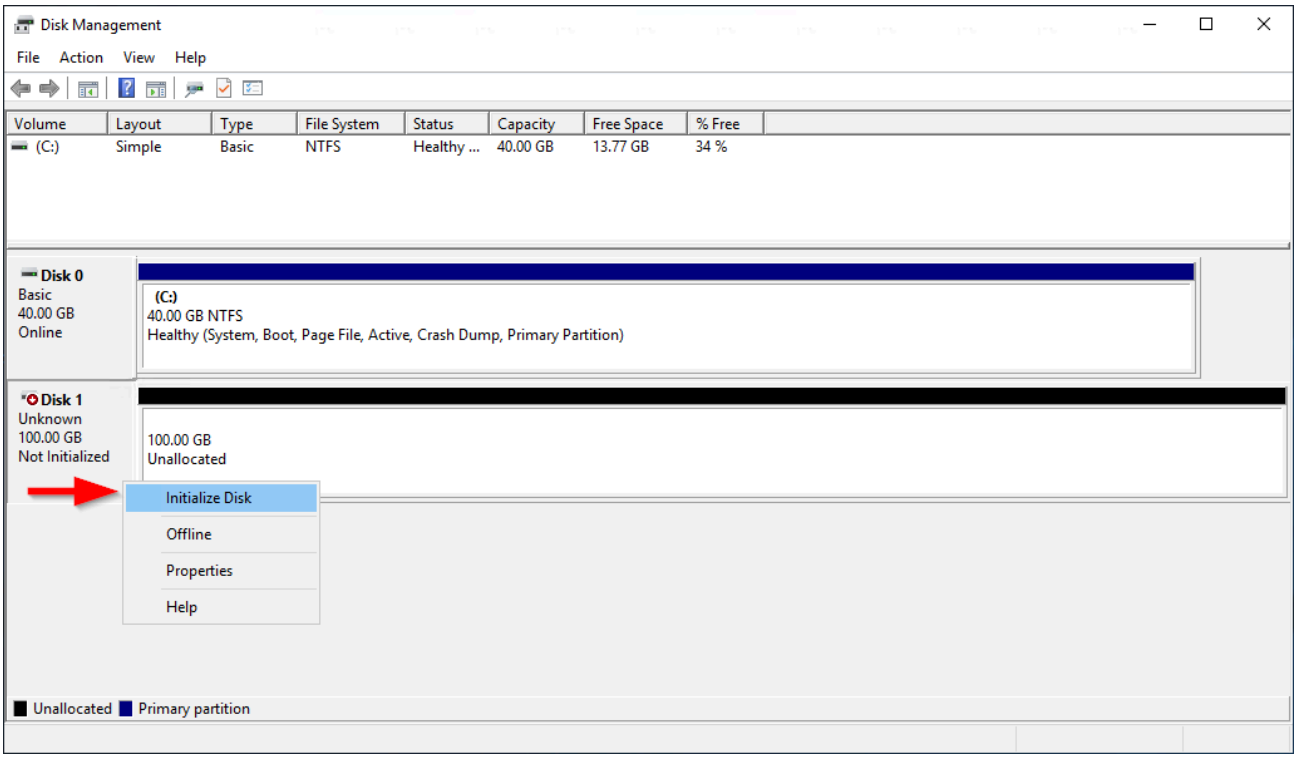


4. (Condicional) Se o disco não estiver inicializado, é necessário inicializar antes de usá-lo. Se o disco já tiver sido inicializado, ignore esta etapa.

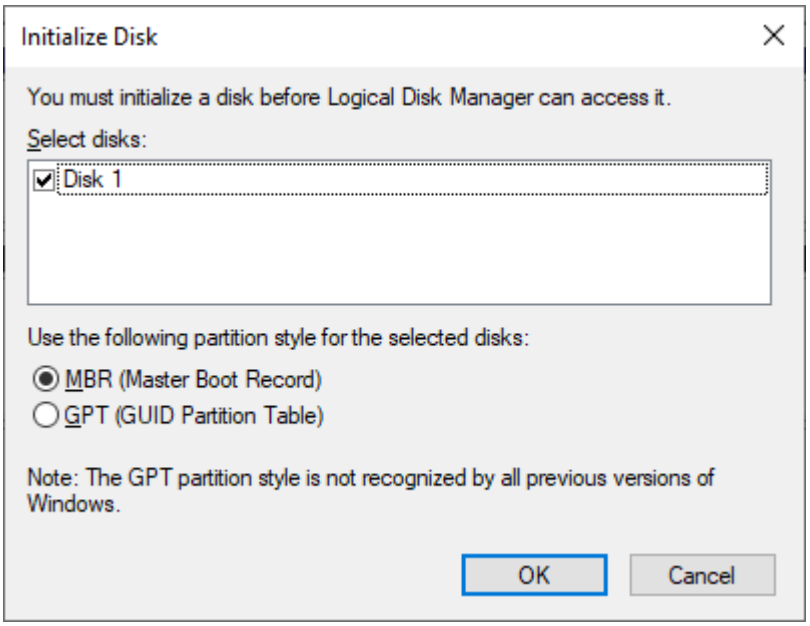
> **Warning**
>
> Se você estiver montando um volume que já tenha dados (por exemplo, um banco de dados públicos ou um volume que você criou a partir de um snapshot), não reformate o volume. Caso contrário, você excluirá os dados existentes.

Se o disco não for inicializado, inicialize-o da seguinte forma:

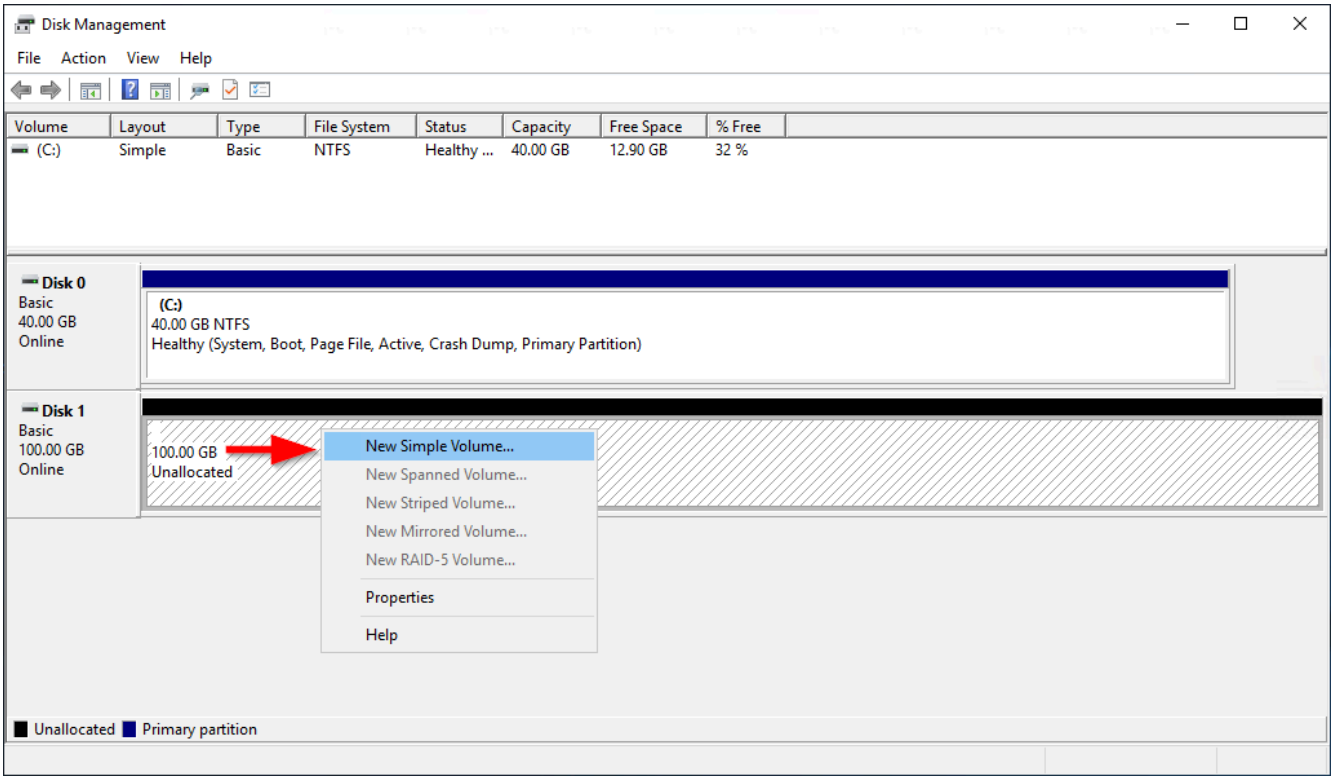
1. Abra o menu de contexto (clique com o botão direito do mouse) no painel esquerdo do disco e escolha Disk Management (Gerenciamento de disco).



2. Na caixa de diálogo Initialize Disk (Inicializar disco), selecione um estilo de partição e escolha OK.

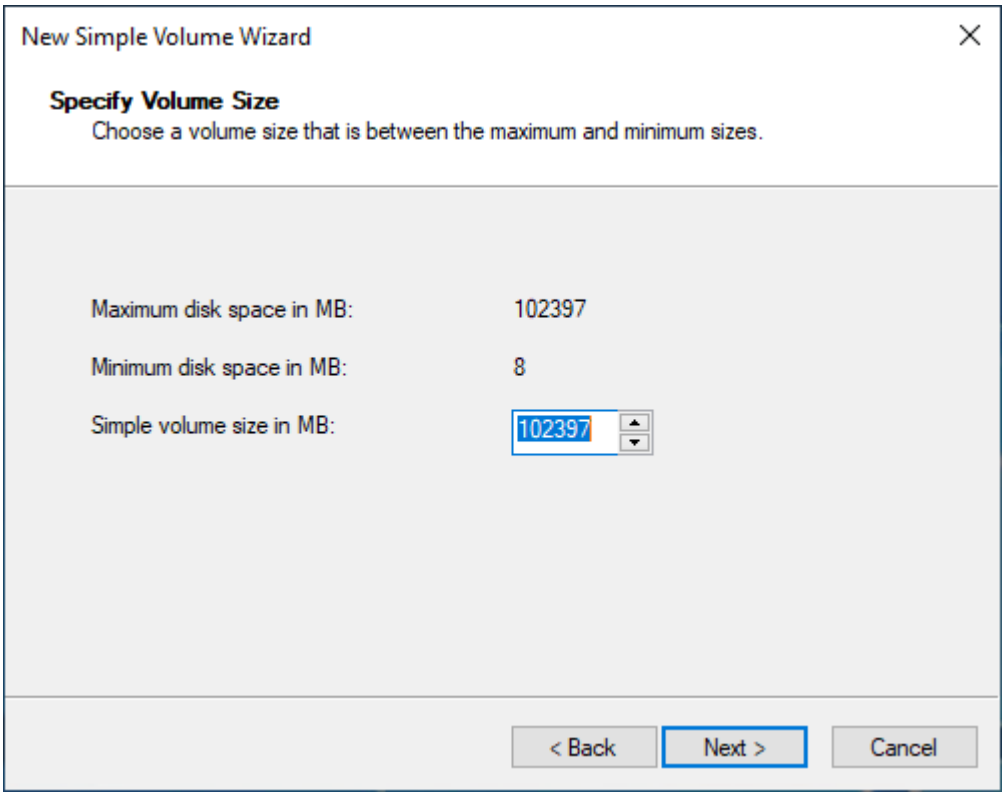


5. Abra o menu de contexto (clique com o botão direito do mouse) no painel direito do disco e escolha New Simple Volume (Novo volume simples).

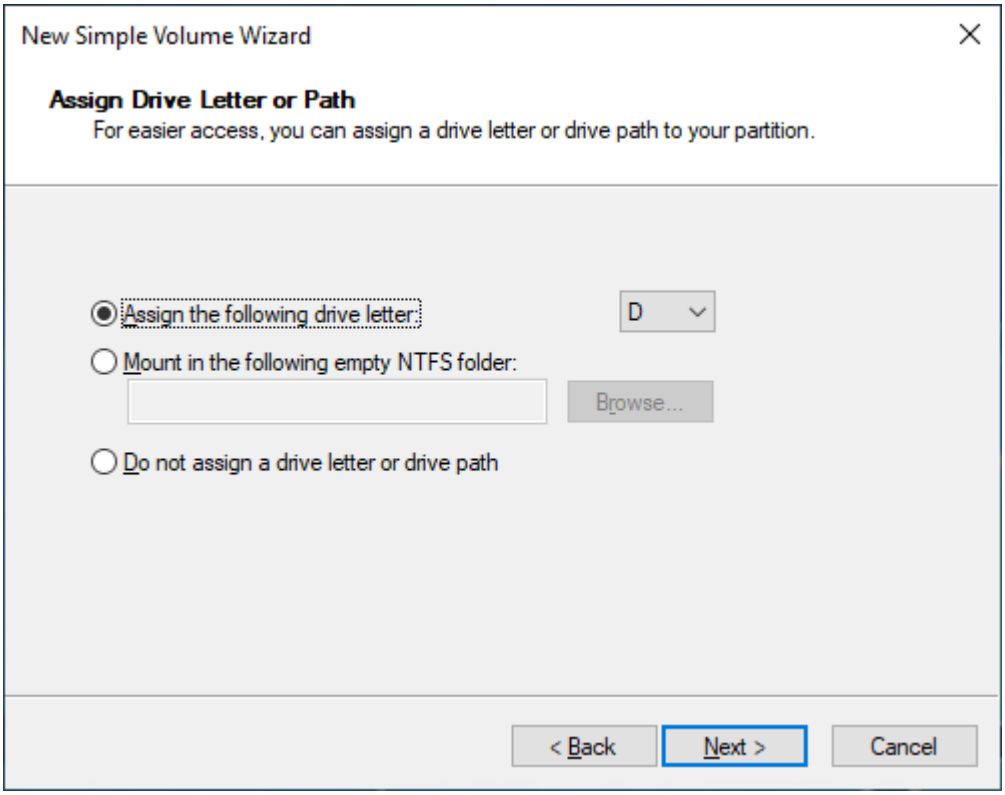


6. No New Simple Volume Wizard (Assistente para novo volume simples), escolha Next (Próximo).

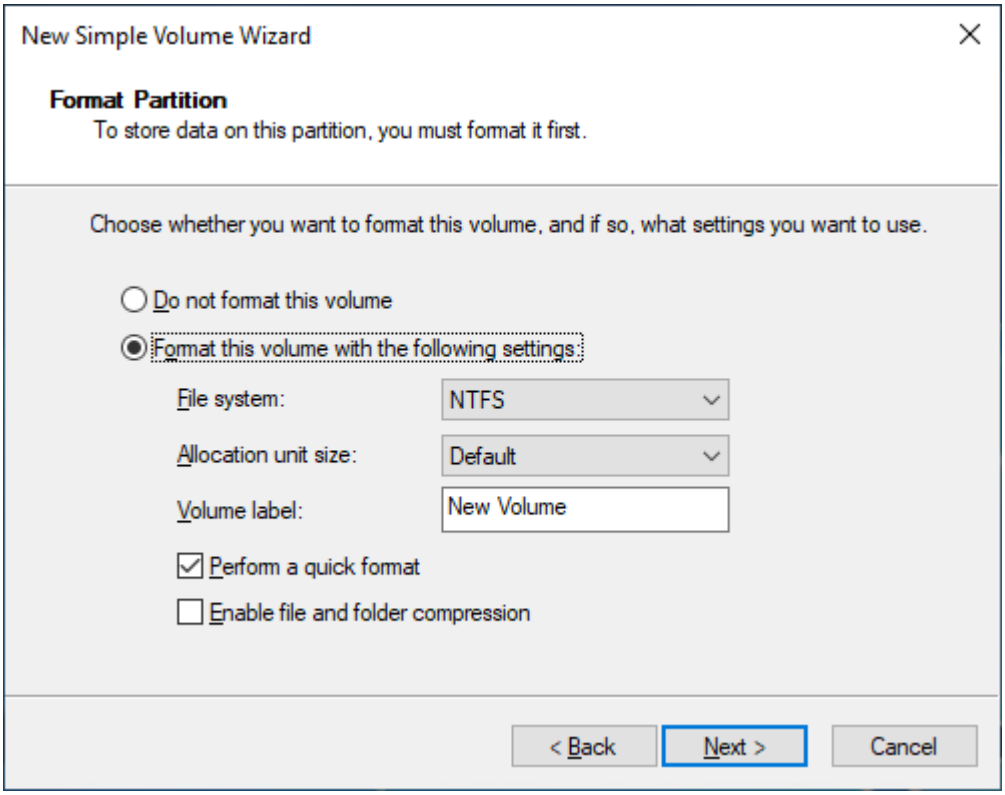
7. Se quiser alterar o valor máximo padrão, especifique o Simple volume size in MB (Tamanho de volume simples em MB) e, depois, escolha Next (Próximo).



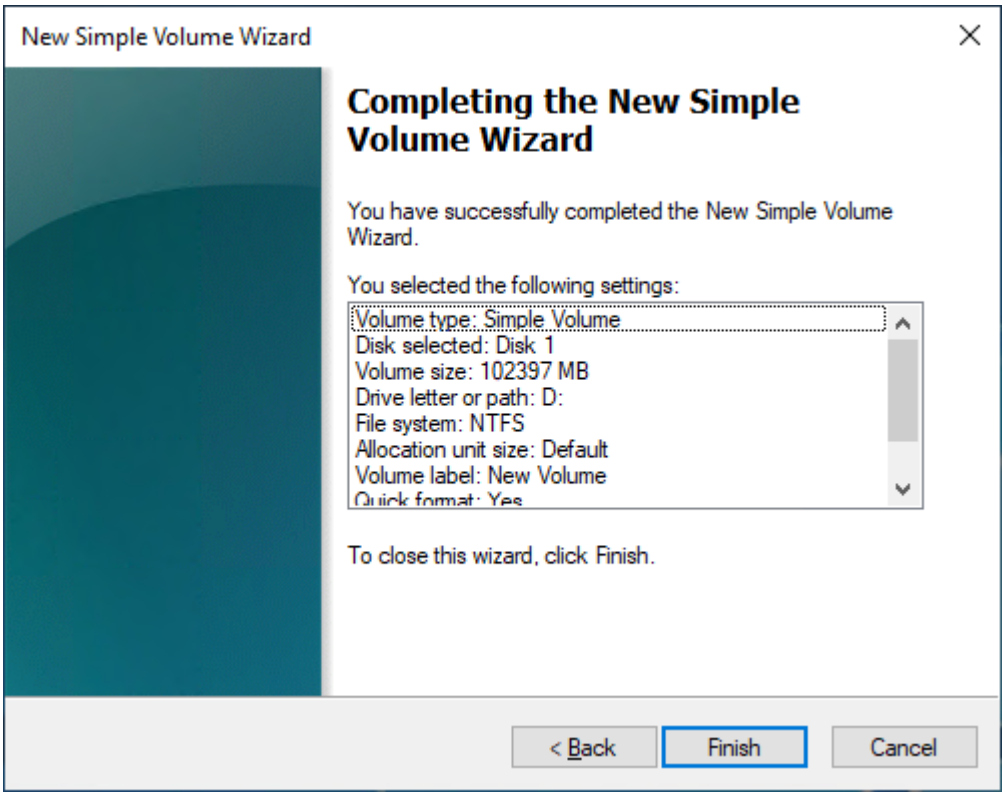
8. Especifique uma letra de unidade preferida, se necessário, na janela suspensa Assign the following drive letter (Atribuir a seguinte letra de unidade) e, em seguida, escolha Next (Próximo).



9. Especifique um Volume Label (Rótulo de volume), ajuste as configurações padrão conforme necessário e, em seguida, escolha Next (Próximo).



10. Revise suas configurações e escolha Finish (Concluir) para aplicar as modificações e fechar o Assistente para novo volume simples.



Visualizar informações sobre um volume do Amazon EBS

É possível visualizar informações descritivas sobre os seus volumes do EBS. Por exemplo, é possível visualizar informações sobre todos os volumes em uma região específica ou visualizar informações detalhadas sobre um único volume, incluindo o tamanho, o tipo de volume, se o volume está criptografado, qual chave do KMS foi usada para criptografá-lo e a instância específica à qual o volume está anexado.

É possível obter informações adicionais sobre os seus volumes do EBS, como, por exemplo, o espaço em disco disponível, no sistema operacional da instância.

Tópicos

- Visualizar informações de volume
- Estados de volumes
- Visualizar métricas de volume
- Visualizar espaço livre em disco

Visualizar informações de volume

É possível visualizar informações sobre um volume usando um dos métodos a seguir.

Console

Para visualizar informações sobre um volume usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Para reduzir a lista, é possível filtrar os volumes usando tags e atributos de volume. Escolha o campo de filtro, selecione uma tag ou um atributo de volume e, depois, selecione o valor do filtro.
4. Para ver mais informações sobre um volume, selecione seu ID.

Como visualizar os volumes do EBS que estão anexados a uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Storage (Armazenamento), a seção Block devices (Dispositivos de blocos) lista os volumes anexados à instância. Para ver informações sobre um volume específico, escolha seu ID na coluna Volume ID (ID do volume).

Amazon EC2 Global View

É possível usar o Amazon EC2 Global View para visualizar seus volumes em todas as regiões para as quais sua conta AWS está habilitada. Para obter mais informações, consulte Amazon EC2 Global View.

AWS CLI

Para visualizar informações sobre um volume do EBS usando o AWS CLI

Use o comando describe-volumes.

Tools for Windows PowerShell

Para visualizar informações sobre um volume do EBS usando as Ferramentas para Windows PowerShell

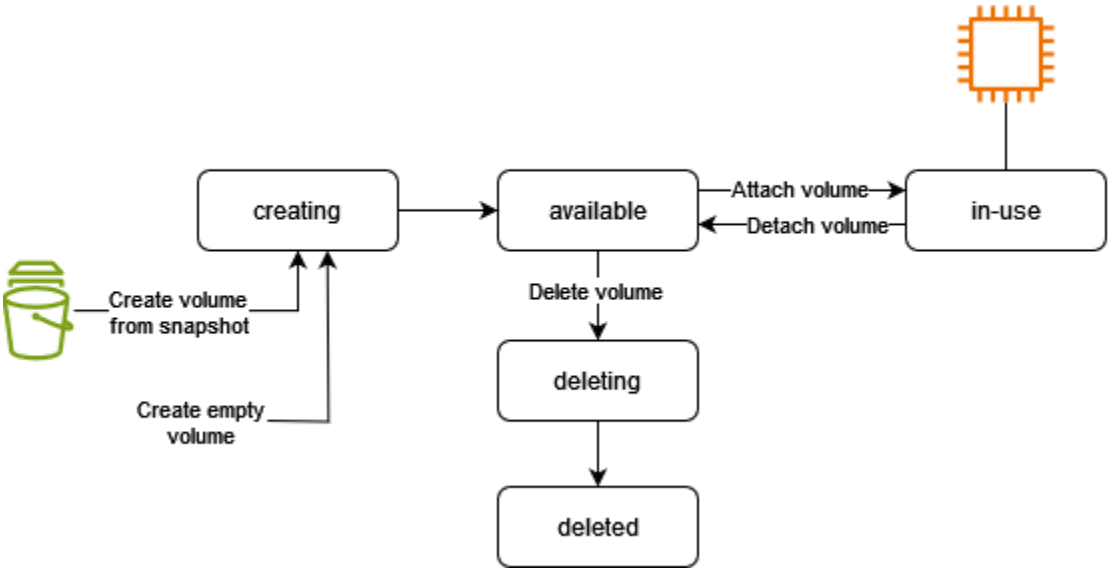
Use o comando Get-EC2Volume.

Estados de volumes

O estado do volume descreve a disponibilidade de um volume do Amazon EBS. Você pode visualizar o estado do volume na coluna Estado na página Volumes no console ou usando o comando AWS CLI describe-volumes.

Um volume do Amazon EBS passa por diferentes estados do momento em que é criado até ser excluído.

A ilustração a seguir mostra as transições entre estados de volumes. É possível criar um volume com base em um snapshot do Amazon EBS ou criar um volume vazio. Quando um volume é criado, ele entra no estado `creating`. Quando o volume estiver pronto para uso, ele entrará no estado `available`. É possível associar um volume disponível a uma instância na mesma zona de disponibilidade do volume. No entanto, é necessário desanexar o volume antes de anexá-lo a uma instância diferente ou excluí-lo. Você poderá excluir um volume quando não precisar mais dele.



A tabela a seguir resume os estados dos volumes.

Estado	Descrição
`creating`	O volume está sendo criado.
`available`	O volume não está anexado a uma instância.

Estado	Descrição
`in-use`	O volume está anexado a uma instância.
`deleting`	O volume está sendo excluído.
`deleted`	O volume foi excluído.
`error`	Houve falha no hardware subjacente relacionado ao volume do EBS e os dados associados ao volume são irrecuperáveis. Para obter informações sobre como restaurar o volume ou recuperar os dados no volume, consulte Meu volume do EBS tem um status de “erro”.

Visualizar métricas de volume

Você pode obter informações adicionais sobre seus volumes do EBS na Amazon CloudWatch. Para ter mais informações, consulte CloudWatch Métricas da Amazon para Amazon EBS.

Visualizar espaço livre em disco

Instâncias do Linux

É possível obter informações adicionais sobre os seus volumes do EBS, como, por exemplo, o espaço em disco disponível, no sistema operacional Linux da instância. Por exemplo, use o comando a seguir:

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

> **Tip**
>
> Você também pode usar o CloudWatch agente para coletar métricas de uso do espaço em disco de uma instância do Amazon EC2 sem se conectar à instância. Para obter mais informações, consulte Criar o arquivo de configuração do CloudWatch agente e Instalar o CloudWatch agente no Guia CloudWatch do usuário da Amazon. Se precisar monitorar o uso do espaço em disco para várias instâncias, você pode instalar e configurar o CloudWatch

agente nessas instâncias usando o Systems Manager. Para obter mais informações, consulte Instalando o CloudWatch agente usando o Systems Manager.

Para obter informações sobre a visualização do espaço livre em disco em uma instância do Windows, consulte Exibir espaço livre em disco no Guia do usuário do Amazon EC2.

Instâncias do Windows

É possível obter informações adicionais sobre os seus volumes do EBS, como, por exemplo, o espaço em disco disponível, no sistema operacional Windows da instância. Por exemplo, é possível visualizar o espaço em disco disponível abrindo o Explorador de Arquivos e selecionando This PC (Este PC).

Também é possível visualizar o espaço em disco disponível usando o comando `dir` a seguir e examinando a última linha da saída:

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

 Directory of C:\

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

Também é possível visualizar o espaço em disco disponível usando o seguinte comando `fsutil`:

```
C:\> fsutil volume diskfree C:
```

```
Total # of free bytes        : 18113204224
Total # of bytes             : 32210153472
Total # of avail free bytes  : 18113204224
```

> **Tip**
>
> Você também pode usar o CloudWatch agente para coletar métricas de uso do espaço em disco de uma instância do Amazon EC2 sem se conectar à instância. Para obter mais informações, consulte Criar o arquivo de configuração do CloudWatch agente e Instalar o CloudWatch agente no Guia CloudWatch do usuário da Amazon. Se precisar monitorar o uso do espaço em disco para várias instâncias, você pode instalar e configurar o CloudWatch agente nessas instâncias usando o Systems Manager. Para obter mais informações, consulte Instalando o CloudWatch agente usando o Systems Manager.

Para obter informações sobre a visualização do espaço livre em disco em uma instância Linux, consulte Exibir espaço livre em disco no Guia do usuário do Amazon EC2.

Modificar um volume do EBS usando Volumes Elásticos do Amazon EBS

É possível aumentar o tamanho dos volumes elásticos do Amazon EBS, alterar o tipo de volume ou ajustar a performance de seus volumes do EBS. Se a sua instância oferecer suporte aos Elastic Volumes, será possível fazê-lo sem desanexar o volume ou reiniciar a instância. Isso permite que você continue usando sua aplicação enquanto as alterações entram em vigor.

Não há cobrança para modificar a configuração de um volume. Você será cobrado pela configuração de novo volume após o início da modificação do volume. Para obter mais informações, consulte a página de Definição de preço do Amazon EBS.

Conteúdo

Requisitos para modificações de volumes do EBS

Os seguintes requisitos e limitações se aplicam quando você modifica um volume do Amazon EBS. Para saber mais sobre o os requisitos gerais para volumes do EBS, consulte Restrições de tamanho e configuração de um volume do EBS.

Tópicos

Tipos de instâncias compatíveis

Elastic Volumes são compatíveis com as seguintes instâncias:

- Todas as instâncias da geração atual
- As seguintes instâncias da geração anterior: C1, C3, C4, G2, I2, M1, M3, M4, R3 e R4

Se o tipo de instância não oferecer suporte a Elastic Volumes, consulte Modificar um volume do EBS se não houver suporte para Elastic Volumes.

Sistema operacional

Os seguintes requisitos do sistema operacional se aplicam:

Linux

As AMIs do Linux exigem uma tabela de partição GUID (GPT) e GRUB 2 para volumes de inicialização de 2 TiB (2048 GiB) ou maiores. Muitas AMIs do Linux atualmente ainda usam o esquema de particionamento de MBR, que só é compatível com tamanhos de volume de inicialização de 2 TiB. Se sua instância não for inicializada com um volume de inicialização superior a 2 TiB, a AMI que você está usando pode ser limitada a um tamanho de volume de inicialização inferior a 2 TiB. Volumes de não inicialização não têm essas limitações nas instâncias do Linux. Para requisitos que afetam os volumes do Windows, consulte Requisitos para volumes do Windows no Guia do usuário do Amazon EC2.

Antes de tentar redimensionar um volume de inicialização além de 2 TiB, é possível determinar se o volume está usando particionamento MBR ou GPT ao executar o seguinte comando na sua instância:

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

Uma instância Amazon Linux com particionamento GPT retorna as seguintes informações:

```
GPT fdisk (gdisk) version 0.8.10

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

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

Uma instância SUSE com particionamento MBR retorna as seguintes informações:

```
GPT fdisk (gdisk) version 0.8.8

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

Windows

Por padrão, o Windows inicializa volumes com uma tabela de partição do registro mestre de inicialização (MBR). Como o MBR é compatível apenas com volumes menores que 2 TiB (2.048 GiB), o Windows impede você de redimensionar volumes MBR para além desse limite. Nesse caso, a opção Extend Volume (Estender volume) é desabilitada no utilitário Disk Management (Gerenciamento de disco) do Windows. Se você usar o AWS Management Console ou AWS CLI para criar um volume particionado por MBR que exceda o limite de tamanho, o Windows não poderá detectar ou usar o espaço adicional. Para requisitos que afetam volumes Linux, consulte Requisitos para volumes Linux no Guia do usuário do Amazon EC2.

Para superar esse limite, é possível criar um novo volume maior com uma tabela de partição de GUID (GPT) e copiar sobre os dados a partir do volume MBR original.

Para criar um volume GPT

1. Crie um o novo volume vazio do tamanho desejado na zona de disponibilidade da instância do EC2 e anexe-o à sua instância.

   > **Note**
   >
   > O novo volume não deve estar em um volume restaurado de um snapshot.

2. Faça login em seu sistema Windows e abra o Gerenciamento de disco (diskmgmt.exe).
3. Abra o menu de contexto (clique com o botão direito do mouse) do novo disco e escolha Online.
4. Na janela Inicializar disco, selecione o novo disco e escolha GPT (tabela de partição GUID), OK.
5. Quando a inicialização estiver concluída, copie os dados do volume original para o novo volume usando uma ferramenta como robocopy ou teracopy.
6. Em Gerenciamento de disco, altere as letras das unidades para os valores apropriados e coloque o antigo volume no modo offline.
7. No console do Amazon EC2, desanexe o volume da instância, reinicie a instância para verificar se ela funciona corretamente, e exclua o antigo volume.

Limitações

- Há limites para o armazenamento agregado máximo que pode ser solicitado em todas as modificações de volume. Para obter mais informações, consulte Cotas de serviço do Amazon EBS no Referência geral da Amazon Web Services.
- Depois de modificar um volume, é necessário aguardar pelo menos seis horas e garantir que o volume esteja no estado `in-use` ou `available` para poder modificar o mesmo volume.
- Modificar um volume do EBS pode levar de alguns minutos a algumas horas, dependendo das alterações de configuração que estão sendo aplicadas. Normalmente, um volume do EBS de 1 TiB pode levar até seis horas para ser modificado. No entanto, o mesmo volume pode levar 24 horas ou mais em outras situações. O tempo necessário para que os volumes sejam modificados nem sempre é escalado linearmente. Portanto, um volume maior pode levar menos tempo e um volume menor pode levar mais tempo.
- Se o volume foi anexado antes de 3 de novembro de 2016, às 23h40 UTC, é necessário inicializar o suporte aos Elastic Volumes. Para obter mais informações, consulte Como inicializar o suporte aos Elastic Volumes.

- Se você encontrar uma mensagem de erro ao tentar modificar em um volume do EBS, ou se estiver modificando um volume do EBS associado a um tipo de instância da geração anterior, obtenha uma das seguintes etapas:
  - Para um volume não raiz, separe o volume da instância, aplique as modificações e reassocie o volume.
  - Para um volume do dispositivo raiz, interrompa a instância, aplique as modificações e reinicie a instância.
- O tempo de modificação é aumentado para volumes que não estão totalmente inicializados. Para obter mais informações, consulte Inicializar volumes de Amazon EBS.
- O novo tamanho do volume não pode exceder a capacidade compatível de seu sistema de arquivos e esquema de particionamento. Para ter mais informações, consulte Restrições de tamanho e configuração de um volume do EBS.
- Se você modificar o tipo de volume de um volume, o tamanho e a performance devem estar dentro dos limites do tipo de volume de destino. Para obter mais informações, consulte Tipos de volume do Amazon EBS
- Não é possível diminuir o tamanho de um volume do EBS. No entanto, você pode criar um volume menor e migrar seus dados para ele usando uma ferramenta em nível de aplicação, como o rsync (instâncias do Linux) ou robocopy (instâncias do Windows).
- Depois de provisionar mais de 32.000 IOPS em um volume `io1` ou `io2` existente, talvez seja necessário desvincular e reanexar o volume ou reiniciar a instância para ver todos os aprimoramentos de performance.
- Os volumes `io2` anexados às instâncias criadas no Nitro System podem ter até 64 TiB de tamanho e até 256.000 IOPS. Os volumes `io2` anexados a outras instâncias podem ter até 16 TiB de tamanho e até 64,000 IOPS, mas só podem alcançar a performance máxima de 32.000 IOPS.
- Não é possível modificar o tipo de volume de volumes `io2` habilitados por Multi-Attach.
- Não é possível modificar o tipo, o tamanho ou as IOPS provisionadas de volumes `io1` habilitados para Multi-Attach.
- Um volume raiz do tipo `io1`, `io2`, `gp2`, `gp3` ou `standard` não pode ser modificado para um volume `st1` ou `sc1`, mesmo que esteja desanexado da instância.
- Embora as instâncias `m3.medium` sejam totalmente compatíveis com a modificação de volume, as instâncias `m3.large`, `m3.xlarge` e `m3.2xlarge` podem não ser compatíveis com todos os recursos da modificação de volume.

Solicitar modificações para seus volumes do EBS

Com os Elastic Volumes, é possível aumentar dinamicamente o tamanho, a performance e o tipo de volume dos volumes do Amazon EBS sem desvinculá-los.

Use o seguinte processo ao modificar um volume:

1. (Opcional) Antes de modificar um volume que contém dados valiosos, a prática recomendada é criar um snapshot de volume caso você precise voltar suas alterações. Para obter mais informações, consulte Criar snapshots de Amazon EBS.
2. Solicite a modificação do volume.
3. Monitore o progresso da modificação do volume. Para obter mais informações, consulte Monitorar o progresso das modificações em volumes do EBS.
4. Se o tamanho do volume tiver sido alterado, estenda o sistema de arquivos de volume para aproveitar o aumento da capacidade de armazenamento. Para ter mais informações, consulte Estender um sistema de arquivos após redimensionar um volume do EBS.

Tópicos

Modificar um volume do EBS usando volumes elásticos

Considerações

Lembre-se do seguinte aomodificar volumes :

- Depois de modificar um volume, é necessário aguardar pelo menos seis horas e garantir que o volume esteja no estado `in-use` ou `available` para poder modificar o mesmo volume.
- Modificar um volume do EBS pode levar de alguns minutos a algumas horas, dependendo das alterações de configuração que estão sendo aplicadas. Normalmente, um volume do EBS de 1 TiB pode levar até seis horas para ser modificado. No entanto, o mesmo volume pode levar 24 horas ou mais em outras situações. O tempo necessário para que os volumes sejam modificados nem sempre é escalado linearmente. Portanto, um volume maior pode levar menos tempo e um volume menor pode levar mais tempo.

- Você não pode cancelar uma solicitação de modificação de volume após ela ter sido enviada.
- Só é possível aumentar o tamanho do volume. Não é possível diminuir o tamanho do volume.
- É possível aumentar ou diminuir a performance do volume.
- Se você não estiver alterando o tipo de volume, as modificações no tamanho e na performance do volume devem estar dentro dos limites do tipo de volume atual. Se você não estiver alterando o tipo de volume, as modificações no tamanho e na performance do volume devem estar dentro dos limites do tipo de volume de destino
- Se você alterar o tipo de volume de `gp2` para `gp3` e não especificar a performance de IOPS ou throughput, o Amazon EBS provisionará automaticamente a performance equivalente à do volume `gp2` de origem ou a performance de `gp3` de linha de base, o que for maior.

  Por exemplo, se você modificar um volume `gp2` de 500 GiB com throughput de 250 MiB/s e 1500 de IOPS para `gp3` sem especificar a performance de IOPS ou throughput, o Amazon EBS provisionará automaticamente o volume `gp3` com 3.000 IOPS (`gp3` IOPS de linha de base) e 250 MiB/s (para corresponder à throughput do volume `gp2` de origem).

Para modificar um volume do EBS, use um dos métodos a seguir.

Console

Para modificar um volume EBS usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume a modificar e escolha Actions (Ações), Modify volume (Modificar volume).
4. A tela Modify volume (Modificar volume) exibe o ID de volume e a configuração atual do volume, incluindo tipo, tamanho, IOPS e throughput. Defina os novos valores de configuração da forma a seguir:
   - Para modificar o tipo, escolha um valor para Volume type (Tipo de volume).
   - Para modificar o tamanho, insira um novo valor para Size (Tamanho).
   - (`gp3` , `io1` e `io2` apenas) Para modificar o valor de IOPS, insira um novo valor para IOPS.
   - (`gp3` apenas) Para modificar a throughput, insira um novo valor para Throughput.
5. Após a alteração das configurações de volume, selecione Modify (Modificar). Quando for solicitada a confirmação, escolha Modify (Modificar).

6.

> **Important**
>
> Se você aumentou o tamanho do volume, também deve estender a partição do volume para usar a capacidade de armazenamento adicional. Para ter mais informações, consulte Estender um sistema de arquivos após redimensionar um volume do EBS.

7. (Somente instâncias do Windows) Se você aumentar o tamanho de um volume NVMe em uma instância que não tenha os drivers AWS NVMe, deverá reinicializar a instância para permitir que o Windows veja o novo tamanho do volume. Para obter mais informações sobre a instalação dos drivers AWS NVMe, consulte Drivers AWS NVMe para instâncias do Windows.

AWS CLI

Para modificar um volume do EBS usando o AWS CLI

Use o comando modify-volume para modificar uma ou mais definições de configuração de um volume. Por exemplo, se você tiver um volume do tipo gp2 com um tamanho de 100 GiB, o comando a seguir alterará a configuração para um volume do tipo `io1` com 10.000 IOPS e um tamanho de 200 GiB.

```
aws ec2 modify-volume --volume-type io1 --iops 10000 --size 200 --volume-
id vol-11111111111111111
```

A seguir está um exemplo de saída:

```
{
    "VolumeModification": {
        "TargetSize": 200,
        "TargetVolumeType": "io1",
        "ModificationState": "modifying",
        "VolumeId": "vol-11111111111111111",
        "TargetIops": 10000,
        "StartTime": "2017-01-19T22:21:02.959Z",
        "Progress": 0,
        "OriginalVolumeType": "gp2",
        "OriginalIops": 300,
        "OriginalSize": 100
```

```
    }
}
```

> **Important**
>
> Se você aumentou o tamanho do volume, também deve estender a partição do volume para usar a capacidade de armazenamento adicional. Para ter mais informações, consulte Estender um sistema de arquivos após redimensionar um volume do EBS.

Inicializar o suporte aos Elastic Volumes (se necessário)

Antes de ser possível modificar um volume que foi anexado a uma instância antes de 3 de novembro de 2016, às 23h40 UTC, é necessário inicializar o suporte à modificação de volumes usando uma das seguintes ações:

- Desanexar e anexar o volume
- Interromper e iniciar a instância

Use um dos procedimentos a seguir para determinar se suas instâncias estão prontas para modificação de volume.

Console

Para determinar se suas instâncias estão prontas usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione o ícone Show/Hide Columns (a engrenagem). Selecione a coluna de atributos Launch time (Tempo de execução) e escolha Confirm (Confirmar).
4. Classifique a lista de instâncias pela coluna Launch Time. Para cada instância iniciada antes da data limite, escolha a guia Storage (Armazenamento) e verifique a coluna Attachment time (Hora da associação) para ver quando os volumes foram anexados.

AWS CLI

Para determinar se suas instâncias estão prontas usando a CLI

Use o comando describe-instances a seguir para determinar se o volume foi anexado antes de 3 de novembro de 2016, às 23h40 UTC.

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

A primeira linha da saída de cada instância mostra o ID dela e se foi iniciada antes da data de interrupção (True ou False). A primeira linha é seguida por uma ou mais linhas que mostram se cada volume do EBS foi anexado antes da data de interrupção (True ou False). No exemplo de saída a seguir, é necessário inicializar a modificação de volume para a primeira instância porque ela foi iniciada antes da data de interrupção e o volume de raiz dela foi anexado antes da data de interrupção. As outras instâncias estão prontas porque foram iniciadas após a data de interrupção.

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

Modificar um volume do EBS se não houver suporte para Elastic Volumes

Se estiver usando um tipo de instância com suporte, será possível utilizar Elastic Volumes para modificar dinamicamente o tamanho, a performance e o tipo de volume dos seus volumes do Amazon EBS sem desanexá-los.

Se não puder usar Elastic Volumes, mas precisar modificar o volume raiz (inicialização), você deverá parar a instância, modificar o volume e reiniciar a instância.

Após a instância ter sido iniciada, é possível verificar o tamanho do sistema de arquivos para ver se sua instância reconhece o espaço de volume maior. No Linux, use o comando df -h para verificar o tamanho do sistema de arquivos.

```
[ec2-user ~]$ df -h
```

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/xvda1            7.9G  943M  6.9G  12% /
tmpfs                 1.9G     0  1.9G   0% /dev/shm
```

Se o tamanho não refletir o volume recém-expandido, amplie o sistema de arquivos do seu dispositivo para que a instância possa usar o novo espaço. Para ter mais informações, consulte Estender um sistema de arquivos após redimensionar um volume do EBS.

Nas instâncias do Windows, talvez seja necessário colocar o volume online para usá-lo. Para ter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso. Você não precisa reformatar o volume.

Monitorar o progresso das modificações em volumes do EBS

Quando você modifica um volume do EBS, ele atravessa uma sequência de estados. O volume insere o estado `modifying`, o estado `optimizing` e, por fim, o estado `completed`. Neste ponto, o volume está pronto para ser modificado ainda mais.

> **Note**
>
> Raramente, uma AWS falha transitória pode resultar em um `failed` estado. Isso não é uma indicação da integridade do volume. Apenas indica que houve falha na modificação do volume. Se isso ocorrer, tente novamente a modificação do volume.

Quando o volume está no estado `optimizing`, sua performance de volume está entre as especificações de configuração de origem e de destino. A performance de volume transitório não será menor que a performance de volume de origem. Se você está fazendo downgrade do IOPS, a performance do volume transitório não é inferior à performance do volume de destino.

As alterações de modificação de volume entram em vigor da seguinte forma:

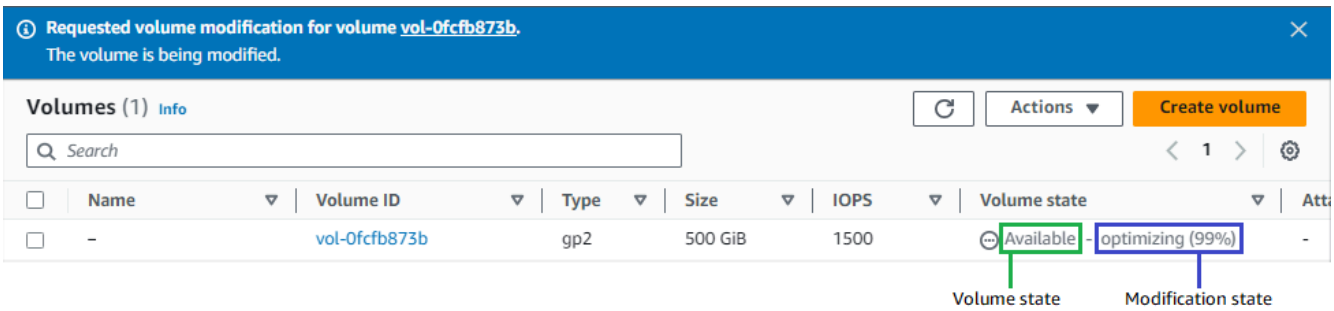
- Alterações de tamanho geralmente demoram alguns segundos para serem concluídas e entram em vigor depois que o volume mudar para o estado `Optimizing`.
- As alterações de performance (IOPS) pode levar de alguns minutos a algumas horas para serem concluídas e dependem das alterações de configuração que estão sendo feitas.
- Em alguns casos, pode demorar até 24 horas para uma nova configuração entrar em vigor, como quando o volume não foi totalmente inicializado. Normalmente, um volume de 1 TiB totalmente usado demora cerca de 6 horas para migrar uma nova configuração de performance.

Use um dos métodos a seguir para monitorar o progresso de uma modificação de volume.

Console

Para monitorar o progresso de uma modificação usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume.
4. A coluna Estado do volume e o campo Estado do volume na guia de Detalhes contêm informações no seguinte formato: *`estado do volume`*: *`estado da modificação`* (*`andamento da modificação`*%). A imagem a seguir mostra o volume e os estados de modificação do volume.



Os possíveis estados de volume são `creating`, `available`, `in-use`, `deleting`, `deleted` e `error`.

Os possíveis estados de modificação são `modifying`, `optimizing` e `completed`.

Depois que a modificação for concluída, somente o estado do volume será exibido. O estado e o progresso da modificação não são mais exibidos.

AWS CLI

Para monitorar o progresso de uma modificação usando o AWS CLI

Use o comando describe-volumes-modifications para visualizar o progresso de uma ou mais modificações de volume. O exemplo a seguir descreve as modificações de volume para dois volumes.

```
aws ec2 describe-volumes-modifications --volume-
ids vol-11111111111111111 vol-22222222222222222
```

Na saída de exemplo a seguir, as modificações de volume ainda estão no estado `modifying`. O andamento é relatado como uma porcentagem.

```
{
    "VolumesModifications": [
        {
            "TargetSize": 200,
            "TargetVolumeType": "io1",
            "ModificationState": "modifying",
            "VolumeId": "vol-11111111111111111",
            "TargetIops": 10000,
            "StartTime": "2017-01-19T22:21:02.959Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 100
        },
        {
            "TargetSize": 2000,
            "TargetVolumeType": "sc1",
            "ModificationState": "modifying",
            "VolumeId": "vol-22222222222222222",
            "StartTime": "2017-01-19T22:23:22.158Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 1000
        }
    ]
}
```

O exemplo a seguir descreve todos os volumes com um estado de modificação `optimizing` ou `completed` e filtra e formata os resultados para mostrar somente as modificações iniciadas em ou depois de 1º de fevereiro de 2017:

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

A seguir, um exemplo de saída com informações sobre dois volumes:

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

CloudWatch Events console

Com CloudWatch Eventos, você pode criar uma regra de notificação para eventos de modificação de volume. É possível usar a regra para gerar uma mensagem de notificação usando o Amazon SNS ou invocar uma função do Lambda em resposta a eventos correspondentes. Os eventos são emitidos com base no melhor esforço.

Para monitorar o progresso de uma modificação usando CloudWatch Eventos

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Escolha Eventos, Criar regra.
3. Para Construir padrão de eventos para corresponder a eventos por serviço, escolha Padrão de eventos personalizado.
4. Para Build custom event pattern (Construir padrão de eventos personalizado), substitua o conteúdo pelo seguinte e escolha Save (Salvar).

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

```
}
```

Veja a seguir um exemplo de dados de evento:

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "2017-01-12T21:09:07Z",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
   ],
   "detail": {
      "result": "optimizing",
      "cause": "",
      "event": "modifyVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

Estender um sistema de arquivos após redimensionar um volume do EBS

Após aumentar o tamanho de um volume do EBS, é necessário estender a partição e o sistema de arquivos para o novo tamanho maior. Você poderá fazer isso à medida que o volume entrar no estado `optimizing`.

Antes de começar

- Crie um snapshot do volume, caso precise reverter as alterações. Para ter mais informações, consulte Criar snapshots de Amazon EBS.
- Confirme se o volume foi modificado corretamente e se está no estado `optimizing` ou `completed`. Para obter mais informações, consulte Monitorar o progresso das modificações em volumes do EBS.
- Confirme se o volume está anexado à instância e se está formatado e montado. Para ter mais informações, consulte Formatar e montar um volume anexado.

- (Somente instâncias do Linux) Se você estiver usando volumes lógicos no volume do Amazon EBS, use o Logical Volume Manager (LVM) para estender o volume lógico. Para obter instruções sobre como fazer isso, consulte a seção Estender o volume lógico em Como faço para criar um volume lógico LVM em um volume EBS inteiro? AWS Artigo do Knowledge Center.

Instâncias do Linux

> **Note**
>
> As instruções a seguir demonstram o processo de extensão de sistemas de arquivos XFS e Ext4 para Linux. Para obter informações sobre como estender um sistema de arquivos diferente, consulte sua documentação.

Para estender um sistema de arquivos no Linux, é necessário estender a partição, se houver uma no volume.

Estender o sistema de arquivos de volumes do EBS

Use o procedimento a seguir para estender o sistema de arquivos de um volume redimensionado.

A nomenclatura de dispositivo e partição é diferente para instâncias Xen e instâncias criadas no Nitro System. Para determinar se a instância é baseada em Xen ou em Nitro, use o comando describe-instance-types da AWS CLI da seguinte forma:

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

`nitro` indica que sua instância é baseada em Nitro. `xen` ou `xen-on-nitro` indica que sua instância é baseada em Xen.

Como estender o sistema de arquivos de volumes do EBS

1. Conecte-se à sua instância.
2. Redimensione a partição, se necessário. Para fazer isso:
   a. Verifique se o volume tem uma partição. Use o comando lsblk.

Nitro instance example

No exemplo de saída a seguir, o volume raiz (`nvme0n1`) tem duas partições (`nvme0n1p1` e `nvme0n1p128`), enquanto o volume adicional (`nvme1n1`) não tem partições.

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0   8G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Xen instance example

No exemplo de saída a seguir, o volume raiz (`xvda`) tem uma partição (`xvda1`), enquanto o volume adicional (`xvdf`) não tem partições.

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

Se o volume tiver uma partição, continue o procedimento a partir da etapa a seguir (2b). Se o volume não tiver partições, pule as etapas 2b, 2c e 2d e continue o procedimento a partir da etapa 3.

> **Dica de solução de problemas**
>
> Caso não esteja visualizando o volume na saída do comando, verifique se o volume está anexado à instância e se está formatado e montado.

b. Verifique se é necessário estender a partição. Na saída do comando lsblk da etapa anterior, compare o tamanho da partição e o tamanho do volume.

Se o tamanho da partição for menor que o tamanho do volume, siga para a próxima etapa. Se o tamanho da partição for igual ao tamanho do volume, não será possível estender a partição.

> **Dica de solução de problemas**
>
> Se o volume ainda refletir o tamanho original, confirme se o volume foi modificado corretamente.

c. Estenda a partição. Use o comando growpart e especifique a partição a ser estendida.

Nitro instance example

Por exemplo, para estender uma partição chamada `nvme0n1p1`, use o comando a seguir.

> **Important**
>
> Observe o espaço entre o nome do dispositivo (`nvme0n1`) e o número da partição (1).

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

Xen instance example

Por exemplo, para estender uma partição chamada `xvda1`, use o comando a seguir.

> **Important**
>
> Observe o espaço entre o nome do dispositivo (`xvda`) e o número da partição (1).

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

Dicas de solução de problemas

- `mkdir: cannot create directory '/tmp/growpart.31171': No space left on device FAILED: failed to make temp dir`: indica que não há espaço livre em disco suficiente no volume para que o growpart crie o diretório temporário necessário para realizar o redimensionamento. Libere espaço em disco e tente novamente.
- `must supply partition-number`: indica que você especificou uma partição incorreta. Use o comando lsblk para confirmar o nome da partição e verifique se inseriu um espaço entre o nome do dispositivo e o número da partição.
- `NOCHANGE: partition 1 is size 16773087. it cannot be grown`: indica que a partição já estende todo o volume e não pode ser estendida. Confirme se o volume foi modificado corretamente.

d. Verifique se a partição foi estendida. Use o comando lsblk. O tamanho da partição agora deve ser igual ao tamanho do volume.

Nitro instance example

O exemplo de saída a seguir mostra que o volume (`nvme0n1`) e a partição (`nvme0n1p1`) têm o mesmo tamanho (`16 GB`).

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

Xen instance example

O exemplo de saída a seguir mostra que o volume (`xvda`) e a partição (`xvda1`) têm o mesmo tamanho (`16 GB`).

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
```

```
##xvda1 202:1    0  16G  0 part /
xvdf    202:80   0  24G  0 disk
```

3. Estenda o sistema de arquivos.

   a. Obtenha o nome, o tamanho, o tipo e o ponto de montagem do sistema de arquivos que precisa estender. Use o comando df -hT.

      Nitro instance example

      O exemplo de saída a seguir mostra que o sistema de arquivos `/dev/nvme0n1p1` tem 8 GB de tamanho, seu tipo é `xfs` e seu ponto de montagem é `/`.

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

      Xen instance example

      O exemplo de saída a seguir mostra que o sistema de arquivos `/dev/xvda1` tem 8 GB de tamanho, seu tipo é `ext4` e seu ponto de montagem é `/`.

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

   b. Os comandos para estender o sistema de arquivos diferem conforme o tipo de sistema de arquivos. Escolha o comando correto abaixo com base no tipo de sistema de arquivos observado na etapa anterior.

      - [Sistema de arquivos XFS] Use o comando xfs_growfs e especifique o ponto de montagem do sistema de arquivos observado na etapa anterior.

        Nitro and Xen instance example

        Por exemplo, para estender um sistema de arquivos montado em `/`, use o comando a seguir.

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

> **Dicas de solução de problemas**
>
> - `xfs_growfs: /data is not a mounted XFS filesystem`: indica que você especificou o ponto de montagem incorreto ou que o sistema de arquivos não é XFS. Para verificar o ponto de montagem e tipo de sistema de arquivos, use o comando df -hT.
> - `data size unchanged, skipping`: indica que o sistema de arquivos já estende todo o volume. Se o volume não tiver partições, confirme se o volume foi modificado corretamente. Se o volume tiver partições, verifique se a partição foi estendida, conforme descrito na etapa 2.

- [Sistema de arquivos Ext4] Use o comando resize2fs e especifique o nome do sistema de arquivos observado na etapa anterior.

  Nitro instance example

  Por exemplo, para estender um sistema de arquivos montado chamado `/dev/nvme0n1p1`, use o comando a seguir.

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

  Xen instance example

  Por exemplo, para estender um sistema de arquivos montado chamado `/dev/xvda1`, use o comando a seguir.

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

> **Dicas de solução de problemas**
>
> - `resize2fs: Bad magic number in super-block while trying to open /dev/xvda1`: indica que o sistema de arquivos não é Ext4. Para verificar o tipo de sistema de arquivos, use o comando df -hT.

- `open: No such file or directory while opening /dev/xvdb1`: indica que você especificou uma partição incorreta. Para verificar a partição, use o comando df -hT.
- `The filesystem is already 3932160 blocks long. Nothing to do!`: indica que o sistema de arquivos já estende todo o volume. Se o volume não tiver partições, confirme se o volume foi modificado corretamente. Se o volume tiver partições, verifique se a partição foi estendida, conforme descrito na etapa 2.

- [Outro sistema de arquivos] Consulte a documentação de seu sistema de arquivos para obter instruções.

c. Verifique se o sistema de arquivos foi estendido. Use o comando df -hT e confirme se o tamanho do sistema de arquivos é igual ao tamanho do volume.

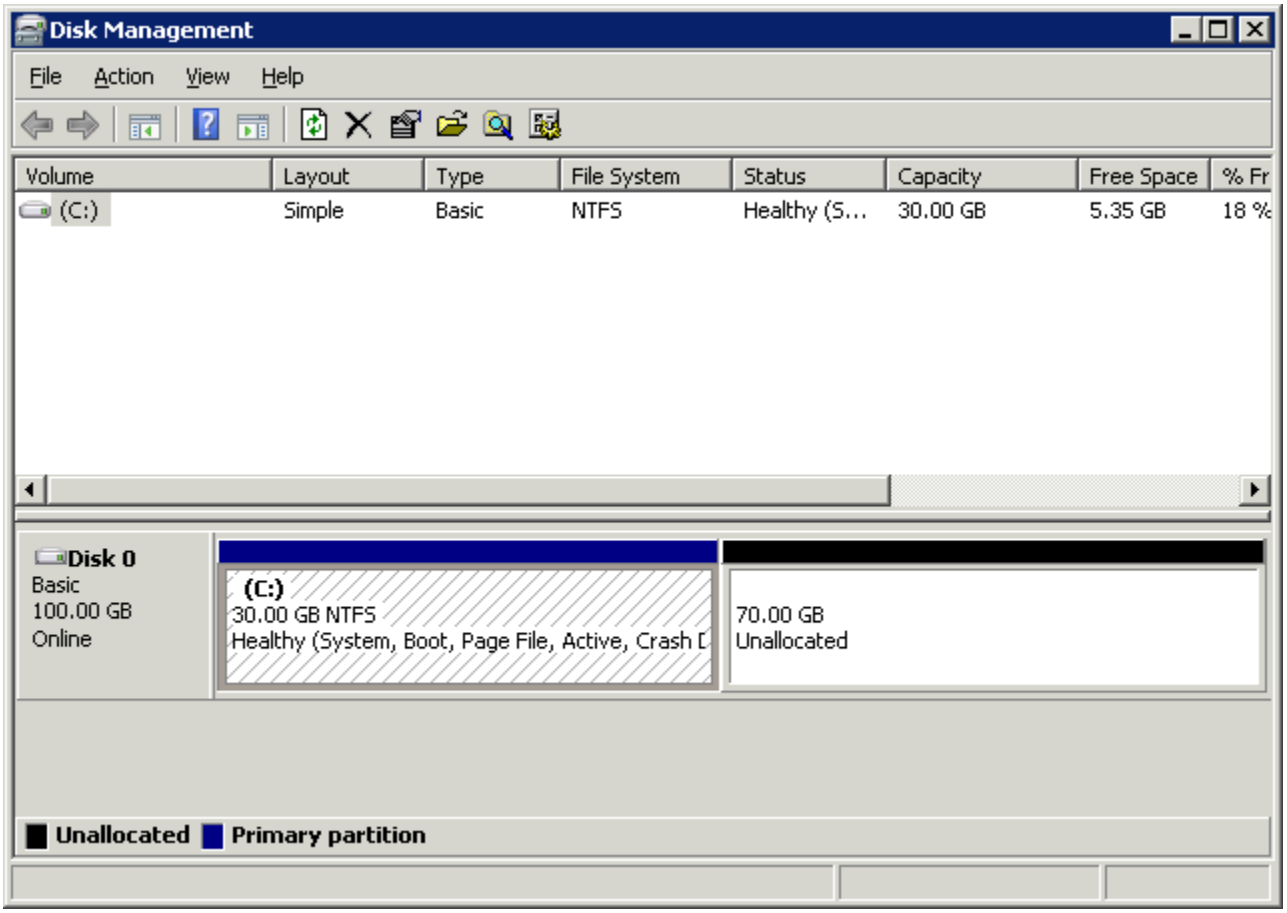
Instâncias do Windows

Use um dos métodos a seguir para estender o sistema de arquivos em uma instância do Windows.

Disk Management utility

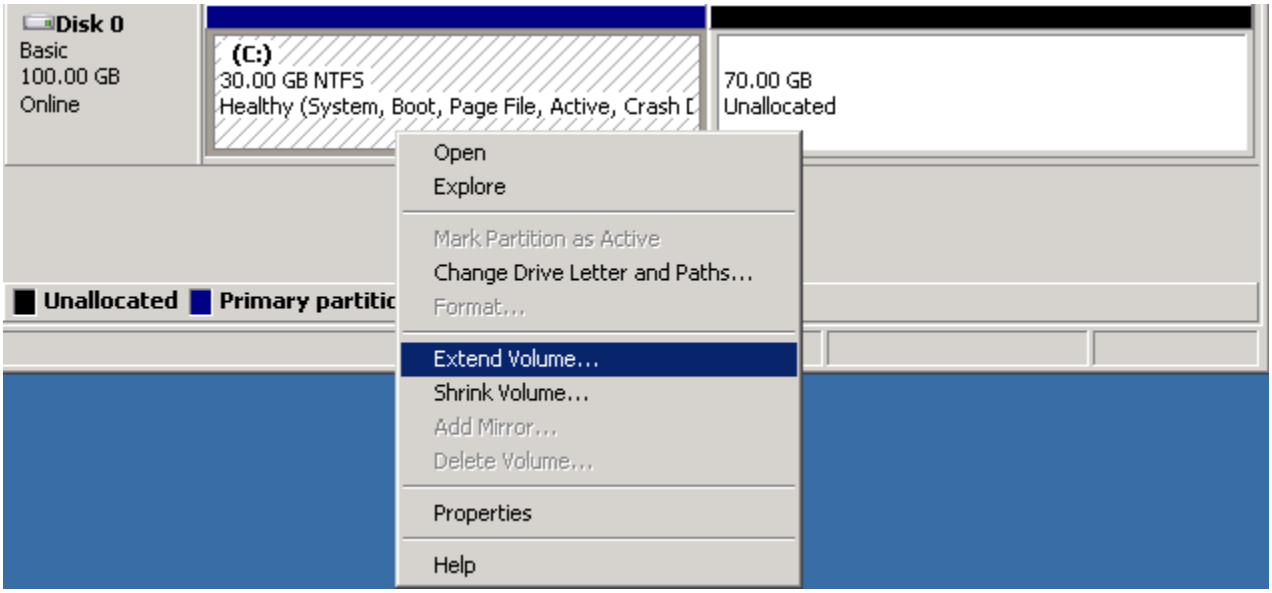
Como estender um sistema de arquivos usando o Gerenciamento de disco

1. Antes de estender um sistema de arquivos que contém dados valiosos, o melhor é criar um snapshot do volume que o contém, caso você precise voltar suas alterações. Para obter mais informações, consulte Criar snapshots de Amazon EBS.
2. Execute a sessão da sua instância do Windows usando o Desktop Remoto.
3. Na caixa de diálogo Run (Executar), digite diskmgmt.msc e pressione Enter. O utilitário de gerenciamento de disco se abre.

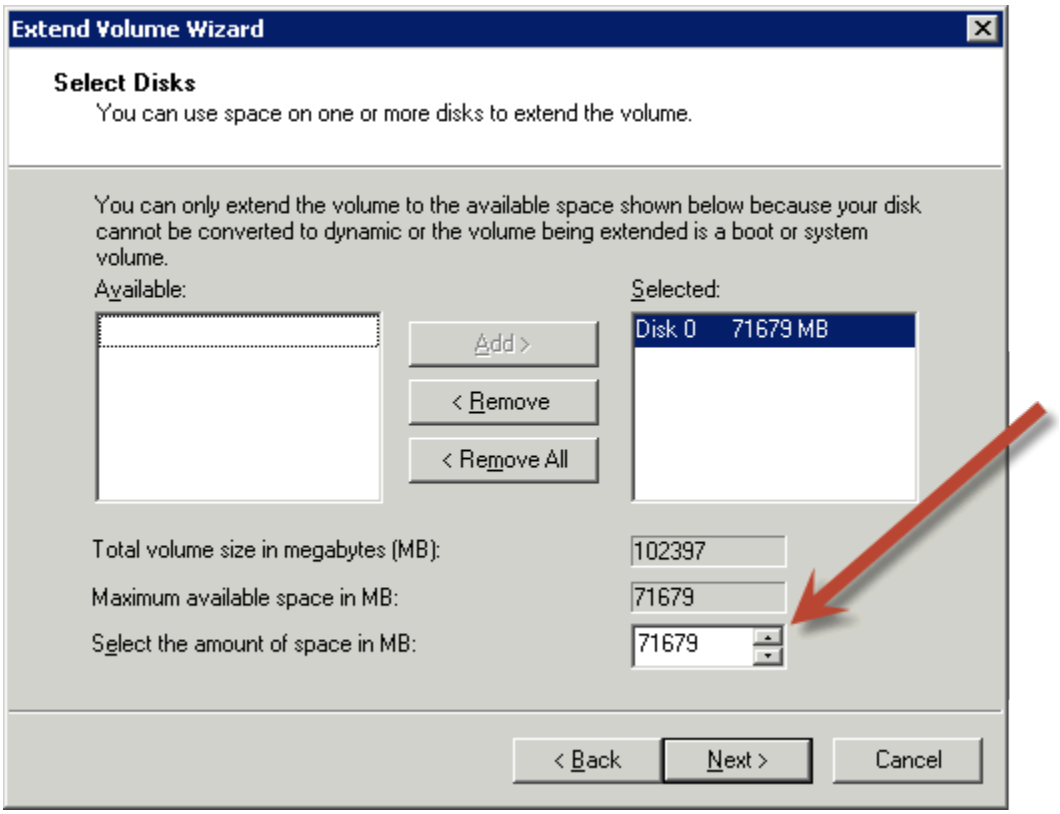


4. No menu Gerenciamento de Disco, escolha Ação, Examinar Discos Novamente.
5. Abra o menu contextual (botão direito do mouse) da unidade expandida e escolha Estender volume.

> **Note**
>
> Extend Volume (Estender volume) pode ser desativado (acinzentado) se:
>
> - O espaço não alocado não é adjacente ao drive. O espaço não alocado deve ser adjacente ao lado direito da unidade que você deseja estender.
> - O volume usa o estilo de partição Master Boot Record (MBR) e já tem 2 TB. Os volumes que usam MBR não podem exceder 2 TB.



6. No assistente Extend Volume (Estender volume), selecione Next (Próximo). Para Selecione o espaço em MB, digite o número de megabytes pelos quais ampliar o volume. Geralmente, você especifica o espaço máximo disponível. O texto destacado em Selected é a quantidade de espaço que será adicionada, não o tamanho final que o volume terá. Assista todo o assistente.



7. Se você aumentar o tamanho de um volume NVMe em uma instância que não tiver o driver do AWS NVMe, reinicie a instância para permitir que o Windows visualize o novo tamanho do volume. Para obter mais informações sobre a instalação do driver AWS NVMe, consulte Drivers AWS NVMe para instâncias do Windows.

PowerShell

Use o procedimento a seguir para estender um sistema de arquivos do Windows usando PowerShell.

Para estender um sistema de arquivos usando PowerShell

1. Antes de estender um sistema de arquivos que contém dados valiosos, o melhor é criar um snapshot do volume que o contém, caso você precise voltar suas alterações. Para obter mais informações, consulte Criar snapshots de Amazon EBS.
2. Faça login na instância do Windows usando o Desktop Remoto.
3. Execute PowerShell como administrador.
4. Execute o `Get-Partition` comando. PowerShell retorna o número da partição correspondente para cada partição, a letra da unidade, o deslocamento, o tamanho e o tipo. Observe a letra da unidade da partição a ser estendida.
5. Execute o seguinte comando para verificar o disco novamente.

```
"rescan" | diskpart
```

6. Execute o comando a seguir, usando a letra da unidade que você anotou na etapa 4 no lugar de**<drive-letter>**. PowerShell retorna o tamanho mínimo e máximo da partição permitida, em bytes.

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

7. Para estender a partição para uma quantidade específica, execute o comando a seguir, inserindo o novo tamanho do volume no lugar de **<size>**. É possível inserir o tamanho em `KB`, `MB` e `GB`, por exemplo, `50GB`.

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

Para estender a partição para o tamanho máximo disponível, execute o seguinte comando.

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

Os PowerShell comandos a seguir mostram o fluxo completo de comandos e respostas para estender um sistema de arquivos a um tamanho específico.

```
PS C:\> Get-Partition


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

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


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

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


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

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

DiskPart has finished scanning your configuration.

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

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


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


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

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


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

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

Os PowerShell comandos a seguir mostram o fluxo completo de comandos e respostas para estender um sistema de arquivos até o tamanho máximo disponível.

```
PS C:\> Get-Partition


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

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


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

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


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

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

DiskPart has finished scanning your configuration.

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

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


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


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

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


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

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

Desanexar um volume do Amazon EBS de uma instância

Você precisa desanexar um volume do Amazon Elastic Block Store (Amazon EBS) de uma instância antes de anexá-lo a uma instância diferente ou excluí-lo. Desanexar um volume não afeta os dados no volume.

Tópicos

- Considerações
- Desmontar e desanexar um volume

- Solução de problemas

Considerações

- É possível separar um volume do Amazon EBS da instância explicitamente ou encerrando a instância. Contudo, se a instância estiver em execução, você deverá primeiro desmontar o volume da instância.
- Se um volume do EBS for o dispositivo raiz de uma instância, você deverá parar a instância antes de separar o volume.
- É possível anexar novamente um volume que foi desanexado (sem desmontá-lo), mas ele talvez não obtenha o mesmo ponto de montagem. Se havia gravações em andamento no volume quando ele foi desanexado, os dados do volume podem não estar sincronizados
- Depois de desanexar um volume, você ainda será cobrado pelo armazenamento de volume, desde que a quantidade de armazenamento exceda o limite do nível AWS gratuito. Exclua um volume para evitar cobranças adicionais. Para obter mais informações, consulte Excluir um volume de Amazon EBS.

Desmontar e desanexar um volume

Use o procedimento a seguir para desmontar e desanexar um volume de uma instância. Isso pode ser útil quando você precisa anexar o volume a uma instância diferente ou quando você precisar excluir o volume.

Etapas

- Etapa 1: desmonte o volume.
- Etapa 2: desanexar o volume da instância.
- Etapa 3: (somente instâncias do Windows) desinstalar os locais de dispositivo offline

Etapa 1: desmonte o volume.

Instâncias do Linux

Na instância do Linux, use o comando a seguir para desmontar o dispositivo `/dev/sdh`.

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

Instâncias do Windows

Na instância do Windows, desmonte o volume, da maneira a seguir.

1. Inicie o utilitário de Gerenciamento de Disco.
   - (Windows Server 2012 e posterior) Na barra de ferramentas, clique com o botão direito do mouse no logo do Windows e escolha Disk Management ((Gerenciamento de disco).
   - (Windows Server 2008) Escolha Start (Iniciar), Administrative Tools (Ferramentas administrativas), Computer Management (Gerenciamento do computador), Disk Management (Gerenciamento de disco).
2. Clique com o botão direito do mouse no disco (por exemplo, clique com o botão direito do mouse em Disk 1 (Disco 1)) e selecione Offline. Aguarde o status do disco ser alterado para Offline antes de abrir o console do Amazon EC2.

Etapa 2: desanexar o volume da instância.

Para desanexar o volume da instância, use um dos seguintes métodos:

Console

Para separar um volume do EBS usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume a ser desvinculado e escolha Actions (Ações), Detach volume (Desvincular volume).
4. Quando a confirmação for solicitada, selecione Detach (Desanexar).

AWS CLI

Para separar um volume do EBS de uma instância usando o AWS CLI

Depois de desmontar o volume, use o comando detach-volume.

Tools for Windows PowerShell

Para separar um volume do EBS de uma instância usando as Ferramentas para Windows PowerShell

Depois de desmontar o volume, use o Dismount-EC2Volumecomando.

Etapa 3: (somente instâncias do Windows) desinstalar os locais de dispositivo offline

Quando você desmonta e desanexa um volume de uma instância, o Windows sinaliza o local do dispositivo como offline. A localização do dispositivo permanece offline após a reinicialização e interromper e reiniciar a instância. Quando você reinicia a instância, o Windows pode montar um dos volumes restantes no local do dispositivo offline. Isso faz com que o volume fique indisponível no Windows. Para evitar que isso aconteça e garantir que todos os volumes estejam conectados a locais de dispositivos online na próxima vez que o Windows for iniciado, execute as seguintes etapas:

1. Na instância, abra o Device Manager (Gerenciador de dispositivos).
2. No Device Manager (Gerenciador de dispositivos), selecione View (Exibir), Show hidden devices (Mostrar dispositivos ocultos).
3. Na lista de dispositivos, expanda o nó Storage controllers (Controladores de armazenamento) .

   Os locais dos dispositivos nos quais os volumes desanexados foram montados são chamados de `AWS NVMe Elastic Block Storage Adapter` e serão mostrados esmaecidos.
4. Clique com o botão direito em cada local de dispositivo esmaecido chamado `AWS NVMe Elastic Block Storage Adapter`, selecione Uninstall device (Desinstalar dispositivo) e escolha Uninstall (Desinstalar).

   > **Important**
   >
   > Não marque a caixa de seleção Delete the driver software for this device (Excluir o software do driver para este dispositivo).

Solução de problemas

A seguir estão problemas comuns encontrados ao separar volumes e como resolvê-los.

> **Note**
>
> Para proteger contra a possibilidade de perda de dados, tire um snapshot do seu volume antes de tentar desmontá-lo. A separação forçada de um volume preso pode causar danos

ao sistema de arquivos ou aos dados que ele contém ou incapacidade de associar um novo volume usando o mesmo nome de dispositivo, a menos que você reinicialize a instância.

- Se você encontrar problemas ao desanexar um volume com o console do Amazon EC2, pode ser útil usar o comando da CLI describe-volumes para diagnosticar o problema. Para obter mais informações, consulte describe-volumes.
- Se seu volume ficar no estado `detaching`, será possível forçar a separação escolhendo Força separação. Use essa opção somente como último recurso para separar um volume de uma instância falha ou se você estiver separando um volume com a intenção de excluí-lo. A instância não tem uma oportunidade de nivelar os caches do sistema de arquivos nem os metadados do sistema de arquivos. Se você usar essa opção, deve executar a verificação do sistema de arquivos e os procedimentos de reparo.
- Caso tenha tentado forçar o volume a separar várias vezes durante vários minutos e ele ficar no estado `detaching`, você pode publicar uma solicitação de ajuda no AWS re:Post. Para ajudar a agilizar uma resolução, inclua o ID do volume e descreva as etapas que já tomou.
- Quando você tenta separar um volume que ainda está montado, o volume pode ficar preso no estado `busy` enquanto está tentando se separar. A seguinte saída de describe-volumes mostra um exemplo dessa condição:

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

Quando você encontra esse estado, a separação poderá ser atrasada indefinidamente até que você desmonte o volume, force a separação, reinicialize a instância ou todos os três.

Excluir um volume de Amazon EBS

Se não precisar mais de um volume do Amazon EBS, é possível excluí-lo. Depois da exclusão, seus dados são excluídos e o volume não pode mais ser conectado a nenhuma instância. Antes de exclusão, é possível armazenar um snapshot do volume, que poderá usar para recriar o volume posteriormente.

> **Note**
>
> Não será possível excluir um volume se ele estiver anexado a uma instância. Para excluir um volume, primeiro é necessário desanexá-lo. Para obter mais informações, consulte Desanexar um volume do Amazon EBS de uma instância.
> É possível verificar se um volume está anexado a uma instância. No console, na página Volumes, é possível visualizar o estado dos volumes.
>
> - Se um volume estiver anexado a uma instância, ele estará no estado `in-use`.
> - Se um volume não estiver anexado a uma instância, ele estará no estado `available`. É possível excluir esse volume.

É possível excluir um volume do EBS usando um dos métodos a seguir.

Console

Para excluir um volume do EBS usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume a ser desvinculado e escolha Actions (Ações), Delete volume (Excluir volume).

   > **Note**
   >
   > Se Delete Volume (Excluir volume) estiver esmaecido, o volume estará anexado a uma instância. Desvincule o volume da instância antes que ele possa ser excluído.

4. Na caixa de diálogo de confirmação, escolha Excluir.

AWS CLI

Para excluir um volume do EBS usando o AWS CLI

Use o comando delete-volume.

Tools for Windows PowerShell

Para excluir um volume do EBS usando as Ferramentas para Windows PowerShell

Use o comando Remove-EC2Volume.

Substituir um volume de Amazon EBS usando um snapshot anterior

Os snapshots do Amazon EBS são a ferramenta de backup preferida do Amazon EC2 devido à sua velocidade, conveniência e custo. Ao criar um volume a partir de um snapshot, você recria seu estado em um ponto específico do tempo com os dados salvos até aquele ponto específico intactos. Ao anexar um volume criado de um snapshot a uma instância, é possível duplicar os dados entre regiões, criar ambientes de teste, substituir um volume de produção danificado ou corrompido em sua totalidade ou recuperar arquivos e diretórios específicos e transferi-los para outro volume anexado. Para ter mais informações, consulte Snapshots do Amazon EBS.

Você pode usar um dos procedimentos a seguir para substituir um volume do Amazon EBS por outro que foi criado a partir de um snapshot anterior desse volume.

Console

Para substituir um volume usando o console

1. Crie um volume usando o snapshot e anote o ID do novo volume. Para ter mais informações, consulte Criar um volume a partir de um snapshot.

   > **Note**
   >
   > Certifique-se criar o volume na mesma zona de disponibilidade da instância. Os volumes só podem ser anexados a instâncias na mesma zona de disponibilidade.

2. Na página Instances (Instâncias), selecione a instância na qual deseja substituir o volume e anote seu ID.

Com a instância ainda selecionada, escolha a guia Storage (Armazenamento). Na seção Block devices (Dispositivos de blocos), localize o volume a ser substituído e anote o nome do dispositivo para o volume, por exemplo `/dev/sda1`.

Escolha o ID do volume.

3. Na tela Volumes, selecione o volume e escolha Actions (Ações), Detach volume (Desvincular volume) e Detach (Desvincular).
4. Selecione o novo volume que você criou na etapa 1 e escolha Actions (Ações), Attach volume (Anexar volume).

   Em Instance (Instância) e Device Name (Nome do dispositivo), insira o ID da instância e o nome do dispositivo que você anotou na etapa 2 e selecione Attach Volume (Anexar volume).
5. Conecte-se à sua instância e monte o volume. Para ter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso.

AWS CLI

Para substituir um volume usando o AWS CLI

1. Crie um novo volume a partir do snapshot. Use o comando create-volume. Em `--snapshot-id`, especifique o ID do snapshot a ser usado. Para `--availability-zone`, especifique a mesma zona de disponibilidade da instância. Configure os demais parâmetros conforme necessário.

   > **Note**
   > Certifique-se criar o volume na mesma zona de disponibilidade da instância. Os volumes só podem ser anexados a instâncias na mesma zona de disponibilidade.

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

   Na saída do comando, anote o ID do novo volume.

2. Obtenha o nome do dispositivo do volume a ser substituído. Use o comando describe-instances. Para `--instance-ids`, especifique o ID da instância na qual deseja substituir o volume.

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

   Em `BlockDeviceMappings` na saída do comando, anote o `DeviceName` e o `VolumeId` do volume a ser substituído.

3. Desanexe da instância o volume a ser substituído. Use o comando detach-volume. Para `--volume-id`, especifique o ID do volume a ser desanexado.

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

4. Anexe o volume de substituição à instância. Use o comando attach-volume. Para `--volume-id`, especifique o ID do volume de substituição. Para `--instance-id`, especifique o ID da instância à qual você deseja anexar o volume. Para `--device`, especifique o mesmo nome de dispositivo que você anotou anteriormente.

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

5. Conecte-se à sua instância e monte o volume. Para ter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso.

Monitorar volumes do Amazon EBS

A AWS fornece automaticamente dados que você pode usar para monitorar seus volumes do Amazon EBS.

Conteúdo

Para obter informações adicionais sobre o monitoramento, consulte CloudWatch Métricas da Amazon para Amazon EBS e Amazon EventBridge para Amazon EBS.

Verificações de status do volume do EBS

As verificações de status de volume permitem que você compreenda, rastreie e gerencie melhor as inconsistências potenciais nos dados em um volume do Amazon EBS. Elas foram desenvolvidas para fornecer as informações necessárias para determinar se os volumes do Amazon EBS estão danificados e para ajudar a controlar como um volume potencialmente inconsistente é manuseado.

As verificações de status de volume são os testes automatizados que executam a cada cinco minutos e retornam um status de êxito ou de falha. Se todas as verificações tiverem êxito, o status do volume será `ok`. Se houve falha em uma verificação, o status do volume será `impaired`. Se o status for `insufficient-data`, as verificações poderão ainda estar em andamento no volume. É possível visualizar os resultados das verificações de status de volume para identificar todos os volumes danificados e tomar as ações necessárias.

Quando o Amazon EBS determina que os dados de um volume estão potencialmente inconsistentes, o padrão é desabilitar a E/S do volume de qualquer instância do EC2 anexada, o que ajuda a evitar a corrupção dos dados. Depois que a E/S está desabilitada, a próxima verificação de status falha, e o status do volume é `impaired`. Além disso, você verá um evento que permite que você saiba que a E/S está desabilitada, e que é possível resolver o status danificado do volume habilitando a E/S para o volume. Aguardamos até que você habilite a E/S para oferecer a oportunidade de decidir se você continuará permitindo que suas instâncias usem o volume ou executem uma verificação de consistência usando um comando, como fsck (instâncias do Linux) ou chkdsk (instâncias do Windows), antes de fazer isso.

> **Note**
>
> O status do volume é baseado nas verificações de status do volume e não reflete o estado do volume. Portanto, o status do volume não indica volumes no estado `error` (por exemplo, quando um volume está incapacitado de aceitar E/S). Para obter informações sobre estados do volume, consulte Estados de volumes.

Se a consistência de um volume específico não for uma preocupação, e você preferir que o volume seja disponibilizado imediatamente se estiver danificado, será possível substituir o comportamento padrão configurando o volume para ativar automaticamente a E/S. Se você ativar o atributo de

volume Auto-EnableIO (`autoEnableIO` na API), a verificação do status do volume continua ser aprovada. Além disso, você verá um evento que permite saber que o volume foi determinado como potencialmente inconsistente, mas que sua E/S foi habilitada automaticamente. Isso permite verificar a consistência do volume ou substituí-lo posteriormente.

A verificação do status da performance de E/S compara a performance do volume real com a performance esperada de um volume. Ele alerta você se o volume estiver com uma performance abaixo das expectativas. Essa verificação de status só está disponível para volumes SSD de IOPS provisionadas (`io1` e `io2`) e SSD de uso geral (`gp3`) anexados a uma instância. A verificação de status não é válida para volumes SSD de uso geral (`gp2`), HDD otimizado para throughput (`st1`), HDD a frio (`sc1`) ou magnéticos (`standard`). A verificação de status de performance de E/S é realizada uma vez a cada minuto e o CloudWatch coleta esses dados a cada cinco minutos. Pode demorar até cinco minutos a partir do momento em que você anexa um volume de `io1` ou `io2` a uma instância para a verificação de status para relatar o status de performance de E/S.

> **Important**
>
> Durante a inicialização dos volumes de Provisioned IOPS SSD que foram restaurados de snapshots, a performance do volume pode ser reduzida a menos de 50% de seu nível esperado, o que faz com que o volume exiba um estado de `warning` na verificação do status de I/O Performance (Performance de E/S). Isso é esperado, e é possível ignorar o estado de `warning` em volumes de Provisioned IOPS SSD enquanto estiver inicializando esses volumes. Para obter mais informações, consulte Inicializar volumes de Amazon EBS.

A tabela a seguir lista os status dos volumes do Amazon EBS.

Status dos volumes	Status de E/S habilitado	Status da performance de E/S (somente volumes **`io1`**, **`io2`** e **`gp3`**)
`ok`	Habilitado (E/S habilitada ou E/S habilitada automatic amente)	Normal (a performance do volume é a esperada)
`warning`	Habilitado (E/S habilitada ou E/S habilitada automatic amente)	Degradado (a performance do volume está abaixo das expectativas)

Status dos volumes	Status de E/S habilitado	Status da performance de E/S (somente volumes **io1**, **io2** e **gp3**)
		Seriamente degradado (a performance do volume está muito abaixo das expectati vas)
`impaired`	Habilitado (E/S habilitada ou E/S habilitada automatic amente) Desabilitado (o volume está offline e com recuperação pendente ou está aguardando o usuário habilitar a E/S)	Paralisado (a performance do volume está severamente impactada) Não disponível (incapaz de determinar a performance da E/S porque a E/S é desabilit ada)
`insufficient-data`	Habilitado (E/S habilitada ou E/S habilitada automatic amente) Dados insuficientes	Dados insuficientes

É possível visualizar e trabalhar com verificações de status usando os seguintes métodos.

Console

Para visualizar verificações de status

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.

   A coluna Volume Status (Status do volume) lista o status operacional de cada volume.
3. Para visualizar os detalhes de status de um volume, selecione-o na grade e escolha a guia Status checks (Verificações de status).
4. Se você tiver um volume com um status de falha em uma verificação de status (o status é `impaired`), consulte Trabalhar com um volume danificado.

Como alternativa, é possível selecionar Events (Eventos) para visualizar todos os eventos de suas instâncias e volumes. Para obter mais informações, consulte Eventos de volume do EBS.

AWS CLI

Para visualizar informações de status do volume

Use o comando describe-volume-status.

Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

Tools for Windows PowerShell

Para visualizar informações de status do volume

Use o comando Get-EC2VolumeStatus.

Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

Eventos de volume do EBS

Por padrão, quando o Amazon EBS determina que os dados de um volume estão potencialmente inconsistentes, ele desabilita a E/S de qualquer instância do EC2 anexada. Isso faz com que a verificação de status do volume falhe e cria um evento de status de volume que indica a causa da falha.

Para habilitar automaticamente a E/S em um volume com dados potencialmente inconsistentes, altere a configuração do atributo do volume Auto-Enabled IO (Habilitar E/S automaticamente) (`autoEnableIO`na API). Para obter mais informações sobre como alterar esse atributo, consulte Trabalhar com um volume danificado.

Cada evento inclui uma hora de início, que indica a hora em que o evento ocorreu, e uma duração, que indica por quanto tempo a E/S do volume foi desabilitada. A hora de término é adicionada ao evento quando a E/S do volume é habilitada.

Os eventos de status de volumes incluem uma das seguintes descrições:

`Awaiting Action: Enable IO`

Os dados do volume estão potencialmente inconsistentes. A E/S é desabilitada para o volume até que você a habilite explicitamente. A descrição do evento é alterada para IO Enabled depois que você habilita a E/S explicitamente.

`IO Enabled`

As operações de E/S foram habilitadas explicitamente para esse volume.

`IO Auto-Enabled`

As operações de E/S foram habilitadas automaticamente nesse volume depois da ocorrência de um evento. Recomendamos verificar as inconsistências dos dados antes de continuar a usar os dados.

`Normal`

Apenas para volumes `io1`, `io2` e `gp3`. A performance do volume é a esperada.

`Degraded`

Apenas para volumes `io1`, `io2` e `gp3`. A performance do volume está abaixo das expectativas.

`Severely Degraded`

Apenas para volumes `io1`, `io2` e `gp3`. A performance do volume está muito abaixo das expectativas.

`Stalled`

Apenas para volumes `io1`, `io2` e `gp3`. A performance do volume está severamente impactada.

É possível visualizar eventos para seus volumes usando os seguintes métodos.

Console

Para visualizar eventos para seus volumes

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events. Todas as instâncias e volumes que têm eventos são listados.
3. É possível filtrar por volume para visualizar somente o status de volumes. Também pode filtrar por tipos específicos de status.

4. Selecione um volume para visualizar seu evento específico.

AWS CLI

Para visualizar eventos para seus volumes

Use o comando describe-volume-status.

Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

Tools for Windows PowerShell

Para visualizar eventos para seus volumes

Use o comando Get-EC2VolumeStatus.

Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

Se você tiver um volume com a E/S desabilitada, consulte Trabalhar com um volume danificado. Se você tiver um volume em que a performance da E/S está abaixo do normal, essa poderá ser uma condição temporária devido a uma ação que você tomou (por exemplo, criar um snapshot de um volume durante o uso de pico, executar o volume em uma instância que não pode oferecer suporte à largura de banda de E/S necessária, acessar dados no volume pela primeira vez etc.).

Trabalhar com um volume danificado

Use as opções a seguir se um volume estiver danificado porque os dados do volume estão potencialmente inconsistentes.

Opções

- Opção 1: executar uma verificação de consistência no volume anexado a sua instância
- Opção 2: executar uma verificação de consistência no volume usando outra instância
- Opção 3. excluir o volume se não precisar mais dele

Opção 1: executar uma verificação de consistência no volume anexado a sua instância

A opção mais simples é habilitar a E/S e executar uma verificação de consistência dos dados no volume enquanto o volume ainda estiver anexado a sua instância do Amazon EC2.

Para executar uma verificação de consistência em um volume anexado

1. Interrompa o uso do volume por todos os aplicativos.
2. Habilite a E/S no volume. Use um dos métodos a seguir.

   Console

   1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   2. No painel de navegação, selecione Events.
   3. Selecione o volume no qual habilitar as operações de E/S.
   4. Escolha Actions (Ações), Enable I/O (Habilitar E/S).

   AWS CLI

   Para habilitar E/S para um volume com a AWS CLI

   Use o comando enable-volume-io.

   Tools for Windows PowerShell

   Para habilitar E/S para um volume com o Tools for Windows PowerShell

   Use o comando Enable-EC2VolumeIO.
3. Verifique os dados no volume.

   a. Execute o comando fsck (instâncias do Linux) ou chkdsk (instâncias do Windows).
   b. (Opcional) Analise todos os logs disponíveis da aplicação ou do sistema para verificar se há mensagens de erro relevantes.
   c. Se o volume estiver insuficiente por mais de 20 minutos, será possível entrar em contato com o AWS Support Center. Escolha Troubleshoot (Solução de problemas) e, na caixa de diálogo Troubleshoot Status Checks (Verificações de status da solução de problemas), escolha Contact Support (Entrar em contato com o suporte) para enviar um caso de suporte.

Opção 2: executar uma verificação de consistência no volume usando outra instância

Use o seguinte procedimento para verificar o volume fora de seu ambiente de produção.

> **Important**
>
> Este procedimento pode causar a perda de E/Ss de gravação que foram suspensas quando a E/S do volume foi desabilitada.

Para executar uma verificação de consistência em um volume isoladamente

1. Interrompa o uso do volume por todas as aplicações.
2. Desanexe o volume da instância. Para obter mais informações, consulte Desanexar um volume do Amazon EBS de uma instância.
3. Habilite a E/S no volume. Use um dos métodos a seguir.

   Console

   1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   2. No painel de navegação, selecione Events.
   3. Selecione o volume que você desanexou na etapa anterior.
   4. Escolha Actions (Ações), Enable I/O (Habilitar E/S).

   AWS CLI

   Para habilitar E/S para um volume com a AWS CLI

   Use o comando enable-volume-io.

   Tools for Windows PowerShell

   Para habilitar E/S para um volume com o Tools for Windows PowerShell

   Use o comando Enable-EC2VolumeIO.
4. Anexe o volume a outra instância. Para obter mais informações, consulte Executar sua instância e Vincular um volume de Amazon EBS a uma instância.
5. Verifique os dados no volume.

   a. Execute o comando fsck (instâncias do Linux) ou chkdsk (instâncias do Windows).

   b. (Opcional) Analise todos os logs disponíveis da aplicação ou do sistema para verificar se há mensagens de erro relevantes.

c. Se o volume estiver insuficiente por mais de 20 minutos, será possível entrar em contato com o AWS Support Center. Escolha Troubleshoot e, em seguida, na caixa de diálogo de solução de problemas, escolha Contact Support para enviar um caso de suporte.

Opção 3. excluir o volume se não precisar mais dele

Se desejar remover o volume do ambiente, simplesmente exclua-o. Para obter informações sobre como excluir um volume, consulte Excluir um volume de Amazon EBS.

Se você tiver um snapshot recente que faça o backup dos dados no volume, será possível criar um novo volume do snapshot. Para obter mais informações, consulte Criar um volume a partir de um snapshot.

Trabalhar com o atributo de volume de E/S habilitada automaticamente

Por padrão, quando o Amazon EBS determina que os dados de um volume estão potencialmente inconsistentes, ele desabilita a E/S de qualquer instância do EC2 anexada. Isso faz com que a verificação de status do volume falhe e cria um evento de status de volume que indica a causa da falha. Se a consistência de um volume específico não for uma preocupação, e você preferir que o volume seja disponibilizado imediatamente se estiver com o status impaired (danificado), será possível substituir o comportamento padrão configurando o volume para ativar automaticamente a E/S. Se você ativar o atributo de volume Auto-Enabled IO (`autoEnableIO` na API), a E/S entre o volume e a instância será reativada e a verificação de status do volume será aprovada. Além disso, você verá um evento que permite que você saiba que o volume estava em um estado de potencialmente inconsistente, mas que sua E/S foi habilitada automaticamente. Quando esse evento ocorre, verifique a consistência do volume e substitui-lo se necessário. Para obter mais informações, consulte Eventos de volume do EBS.

É possível visualizar e modificar o atributo Auto-Enabled IO (E/S habilitado automaticamente) de um volume usando um dos métodos a seguir.

Amazon EC2 console

Para visualizar o atributo de E/S habilitado automaticamente de um volume

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume e escolha a guia Status Checks (Verificações de status).

O campo Auto-Enabled IO (E/S habilitado automaticamente) exibe a configuração atual Enabled (Habilitado) ou Disabled (Desabilitado) do volume selecionado.

Para modificar o atributo de E/S habilitado automaticamente de um volume

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume e escolha Actions (Ações), Manage auto-enabled I/O (Gerenciar E/S habilitada automaticamente).
4. Para habilitar E/S automaticamente para um volume danificado, marque a caixa de seleção Auto-enable I/O for impaired volumes (Habilitar E/S para volumes danificados). Para desabilitar o recurso, limpe a caixa de seleção.
5. Escolha Atualizar.

AWS CLI

Para visualizar o atributo AutoEnableIO de um volume

Use o comando describe-volume-attribute.

Para modificar o atributo autoEnableIO de um volume

Use o comando modify-volume-attribute.

Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

Tools for Windows PowerShell

Para visualizar o atributo AutoEnableIO de um volume

Use o comando Get-EC2VolumeAttribute.

Para modificar o atributo autoEnableIO de um volume

Use o comando Edit-EC2VolumeAttribute.

Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

Testes de falhas no Amazon EBS

Use AWS Fault Injection Service a ação Pausar E/S para interromper temporariamente a E/S entre um volume do Amazon EBS e as instâncias às quais ele está conectado para testar como suas cargas de trabalho lidam com interrupções de E/S. Com AWS FIS, você pode usar experimentos controlados para testar sua arquitetura e monitoramento, como CloudWatch alarmes da Amazon e configurações de tempo limite do sistema operacional, e melhorar a resiliência a falhas de armazenamento.

Para obter mais informações sobre AWS FIS, consulte o Guia AWS Fault Injection Service do usuário.

Considerações

Tenha em mente as seguintes considerações para pausar a E/S do volume:

- Você pode pausar a E/S para todos os tipos de volume do Amazon EBS que estão conectados a instâncias criadas no Nitro System.
- Você pode pausar a E/S para o volume raiz.
- Você pode pausar a E/S para volumes habilitados para Multi-Attach. Se você pausar a E/S de um volume habilitado para Multi-Attach, a E/S será pausada entre o volume e todas as instâncias às quais ele está conectado.
- Para testar a configuração de tempo limite do sistema operacional, defina duração do experimento igual ou maior que o valor especificado para `nvme_core.io_timeout`. Para ter mais informações, consulte Tempo limite de operação de E/S.
- Se você direcionar a E/S para um volume que tenha E/S pausada, acontecerá o seguinte:
  - O status do volume mudará para `impaired` em 120 segundos. Para ter mais informações, consulte Monitorar volumes do Amazon EBS.
  - As CloudWatch métricas para o comprimento da fila (`VolumeQueueLength`) serão diferentes de zero. Qualquer alarme ou monitoramento deve monitorar uma profundidade de fila diferente de zero. Para obter mais informações, consulte Métricas para volumes do Amazon EBS.
  - As CloudWatch métricas para `VolumeReadOps` ou `VolumeWriteOps` serão`0`, o que indica que o volume não está mais processando I/O.

Limitações

Tenha em mente as seguintes limitações para pausar E/S do volume:

- Volumes de armazenamento de instância não são compatíveis.
- Os tipos de instâncias baseadas em Xen não são compatíveis.
- Você não pode pausar a E/S para volumes criados em um posto avançado em AWS Outposts, em uma AWS Wavelength zona ou em uma zona local.

Você pode realizar um experimento básico no console do Amazon EC2 ou pode realizar experimentos mais avançados usando o AWS FIS console. Para obter mais informações sobre como realizar experimentos avançados usando o AWS FIS console, consulte os tutoriais AWS FIS no Guia do AWS Fault Injection Service usuário.

Para realizar um experimento básico usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume para o qual deseja pausar a E/S e escolha Ações, Injeção de falha, Pausar E/S de volume.
4. Em Duração, insira a duração durante a qual pausar a E/S entre o volume e as instâncias. O campo ao lado da lista suspensa Duração mostra a duração no formato ISO 8601.
5. Na seção Acesso ao serviço, selecione a função de serviço do IAM AWS FIS para assumir a realização do experimento. Você pode usar o perfil padrão ou um perfil existente criado por você. Para obter mais informações, consulte Criar um perfil do IAM para experimentos do AWS FIS.
6. Escolha Pausar E/S do volume. Quando solicitado, insira `start` no campo de confirmação e escolha Iniciar experimento.
7. Monitore o progresso e o impacto do seu experimento. Para obter mais informações, consulte Monitorar o AWS FIS no Guia do usuário do AWS FIS .

Snapshots do Amazon EBS

Você pode fazer backup dos dados em seus volumes do Amazon EBS fazendo point-in-time cópias, conhecidas como snapshots do Amazon EBS. Um snapshot é um backup incremental, o que significa que apenas os blocos existentes no dispositivo que mudaram desde o snapshot mais recente são salvos. Isso minimiza o tempo necessário para criar o snapshot e economiza em custos de armazenamento ao não duplicar os dados.

> **Important**
>
> AWS não faz backup automático dos dados armazenados em seus volumes do EBS. Para garantir resiliência dos dados e recuperação de desastres, é sua responsabilidade criar snapshots do EBS regularmente ou configurar a criação automática de snapshots usando o Amazon Data Lifecycle Manager ou o AWS Backup.

Os snapshots do EBS são armazenados no Amazon S3, em buckets do S3 que você não pode acessar diretamente. Você pode criar e gerenciar os snapshots usando o console ou a API do Amazon EC2. Você não pode acessar os snapshots usando o console do Amazon S3 nem a API do Amazon S3.

Cada snapshot contém todas as informações necessárias para restaurar seus dados (desde o momento em que o snapshot foi tirado) até um volume novo do EBS. Quando você cria um volume do EBS baseado em um snapshot, o novo volume começa como uma réplica exata do volume original que foi usado para criar o snapshot. O volume replicado carrega dados em segundo plano, por isso é possível começar a usá-lo imediatamente. Se você acessar dados que ainda não foram carregados, o volume imediatamente baixa os dados solicitados do Amazon S3 e continua carregando o restante dos dados de volume em segundo plano. Para obter mais informações, consulte Criar snapshots de Amazon EBS. Ao excluir um snapshot, somente os dados exclusivos desse snapshot serão removidos. Para ter mais informações, consulte Excluir um snapshot do Amazon EBS.

Para obter mais informações, consulte a página do produto Snapshots do Amazon EBS.

Eventos de snapshot

Você pode acompanhar o status dos seus snapshots do EBS por meio CloudWatch de Eventos. Para ter mais informações, consulte Eventos de snapshot do EBS.

Snapshots consistentes com aplicações (somente instâncias do Windows)

Usando o Run Command do Systems Manager, é possível gerar snapshots consistentes com a aplicação de todos os volumes do EBS anexados às instâncias do Amazon EC2 no Windows. O processo de snapshot usa o Serviço de Cópias de Sombra de Volume (VSS) do Windows para fazer backups no nível da imagem das aplicações que reconhecem o VSS, incluindo os dados de transações pendentes entre essas aplicações e o disco. Você não precisa desligar as instâncias ou desconectá-las ao fazer backup de todos os volumes anexados. Para obter mais informações, consulte Criar um snapshot consistente com aplicações VSS.

Snapshots de vários volumes

Os snapshots podem ser usados para criar um backup de workloads essenciais, como um banco de dados grande ou um sistema de arquivos que engloba vários volumes do EBS. Os instantâneos de vários volumes permitem que você tire instantâneos exatos point-in-time, coordenados com dados e consistentes em falhas em vários volumes do EBS conectados a uma instância do EC2. Você não precisa mais interromper a instância ou coordenar entre volumes para garantir consistência em caso de falha, pois os snapshots são tirados automaticamente em vários volumes do EBS. Para obter mais informações, consulte as etapas para criar um snapshot de volume do EBS em Criar snapshots de Amazon EBS.

Definição de preço de snapshot

As cobranças dos seus snapshots são baseadas na quantidade de dados armazenados. Como os snapshots são incrementais, a exclusão de um snapshot pode não reduzir os custos de armazenamento de dados. Os dados referenciados exclusivamente por um snapshot são removidos quando esse snapshot é excluído, mas os dados referenciados por outros snapshots são preservados. Para obter mais informações, consulte Volumes e snapshots do Amazon Elastic Block Store no Manual do usuário do AWS Billing .

Conteúdo

- Bloquear o acesso público aos snapshots
- Lixeira de snapshots
- Amazon EBS local snapshots on Outposts

Como funcionam os snapshots

O primeiro snapshot criado por você a partir de um volume será sempre um snapshot completo. Ele inclui todos os blocos de dados gravados no volume no momento da criação do snapshot. Os snapshots subsequentes do mesmo volume são snapshots incrementais. Eles incluem apenas blocos de dados alterados e novos gravados no volume desde a criação do último snapshot

O tamanho de um snapshot completo é determinado pelo tamanho dos dados cujo backup está sendo feito, não pelo tamanho do volume de origem. Da mesma forma, os custos de armazenamento associados a um snapshot completo são determinados pelo tamanho do snapshot, não pelo tamanho do volume de origem. Por exemplo, você cria o primeiro snapshot de um volume de `200 GiB` do Amazon EBS que contém apenas `50 GiB` de dados. Isso resulta em um snapshot completo com tamanho de `50 GiB` e você será cobrado pelo armazenamento de snapshot de `50 GiB`.

Da mesma forma, o tamanho e os custos de armazenamento de um snapshot incremental são determinados pelo tamanho de todos os dados gravados no volume desde a criação do snapshot anterior. Continuando este exemplo, se você criar um segundo snapshot do volume de `200 GiB` após a alteração de `20 GiB` de dados e a adição de `10 GiB` de dados, o instantâneo incremental terá tamanho de `30 GiB`. Você será então cobrado por esse armazenamento de snapshot adicional de`30 GiB`.

Para obter mais informações sobre preços de snapshot, consulte Definição de preço do Amazon EBS.

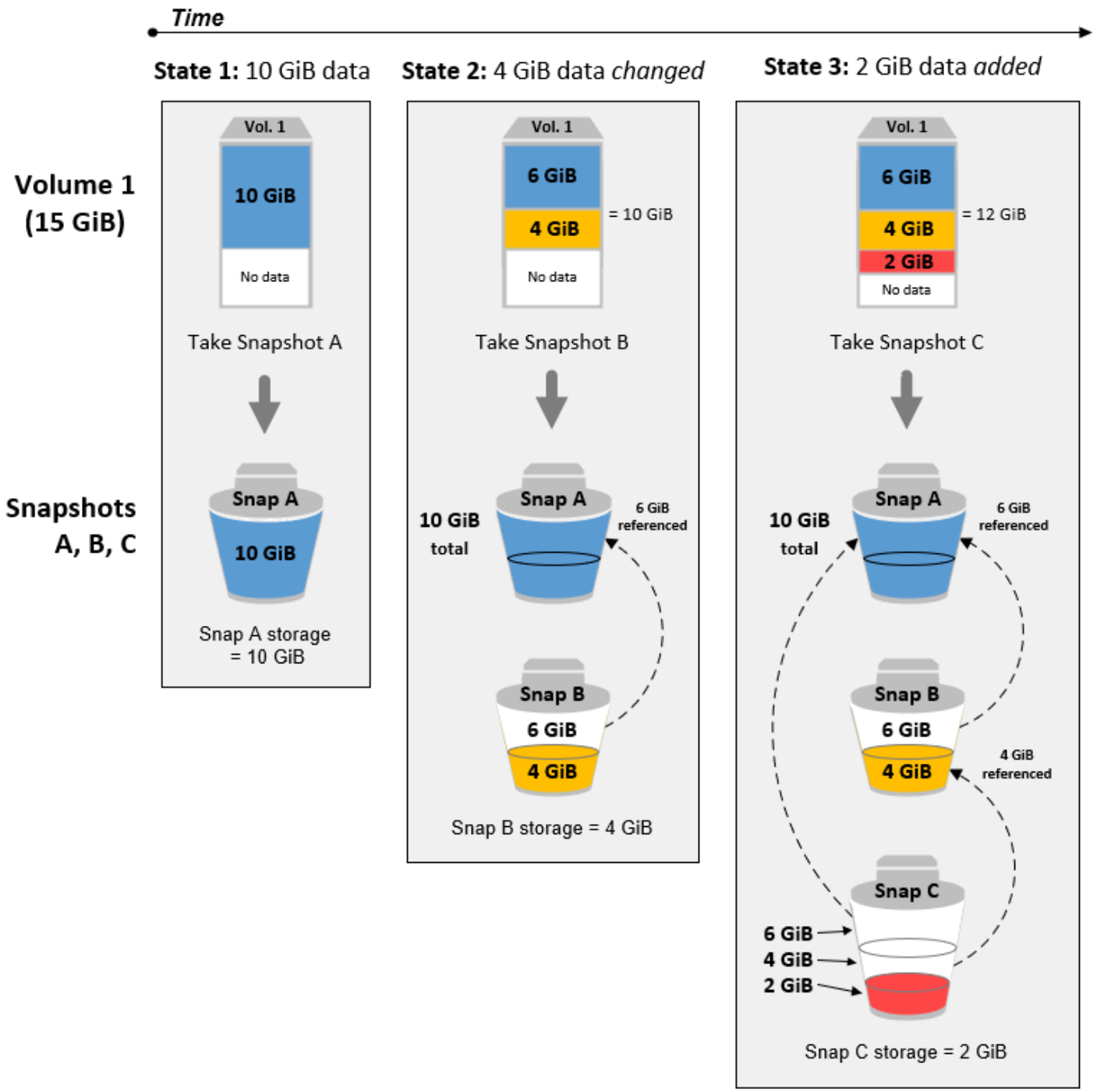
> **Important**
>
> Quando você arquiva um snapshot incremental, ele é convertido em um snapshot completo que inclui todos os blocos gravados no volume no momento em que o snapshot foi criado. Em seguida, ele é movido para o nível de arquivamento de snapshots do Amazon EBS. Os snapshots no nível de arquivamento são cobrados a uma taxa diferente dos snapshots no nível padrão. Para ter mais informações, consulte Definição de preço e faturamento.

As seções a seguir mostram como um snapshot do EBS captura o estado de um volume em um ponto no tempo e como snapshots sucessivos de um volume em constante mudança criam um histórico dessas alterações.

Vários snapshots do mesmo volume

O diagrama nesta seção mostra o Volume 1, que tem tamanho de `15 GiB` em três pontos no tempo. Um snapshot é retirado de cada um desses três estados de volumes. O diagrama mostra especificamente o seguinte:

- No Estado 1, o volume tem `10 GiB` de dados. O Snap A é o primeiro snapshot criado do volume. O Snap A é um instantâneo completo e todos os de `10 GiB` dados são copiados.
- No Estado 2, o volume ainda contém `10 GiB` de dados, mas apenas `4 GiB` foram alterados depois que o Snap A foi feito. O Snap B é um instantâneo incremental. Ele precisa fazer backup apenas dos `4 GiB` que foram alterados. Os outros `6 GiB` de dados inalterados, que já estão copiados e armazenados no Snap A, são referenciados pelo Snap B em vez de copiados novamente. Isso é indicado pela seta tracejada.
- No Estado 3, `2 GiB` de dados foram adicionados ao volume, totalizando `12 GiB`, depois que o Snap B foi feito. O Snap C é um instantâneo incremental. Ele precisa fazer backup apenas dos `2 GiB` que foram adicionados depois que o Snap B ser tomado. Como mostrado pelas setas tracejadas, o Snap C faz referência aos `4 GiB` de dados armazenados no Snap B e aos `6 GiB` de dados armazenados no Snap A.
- O armazenamento total necessário para os três snapshots é de `16 GiB`. Isso representa 10 GiB para o Snap A, 4 GiB para o Snap B e 2 GiB para o Snap C.



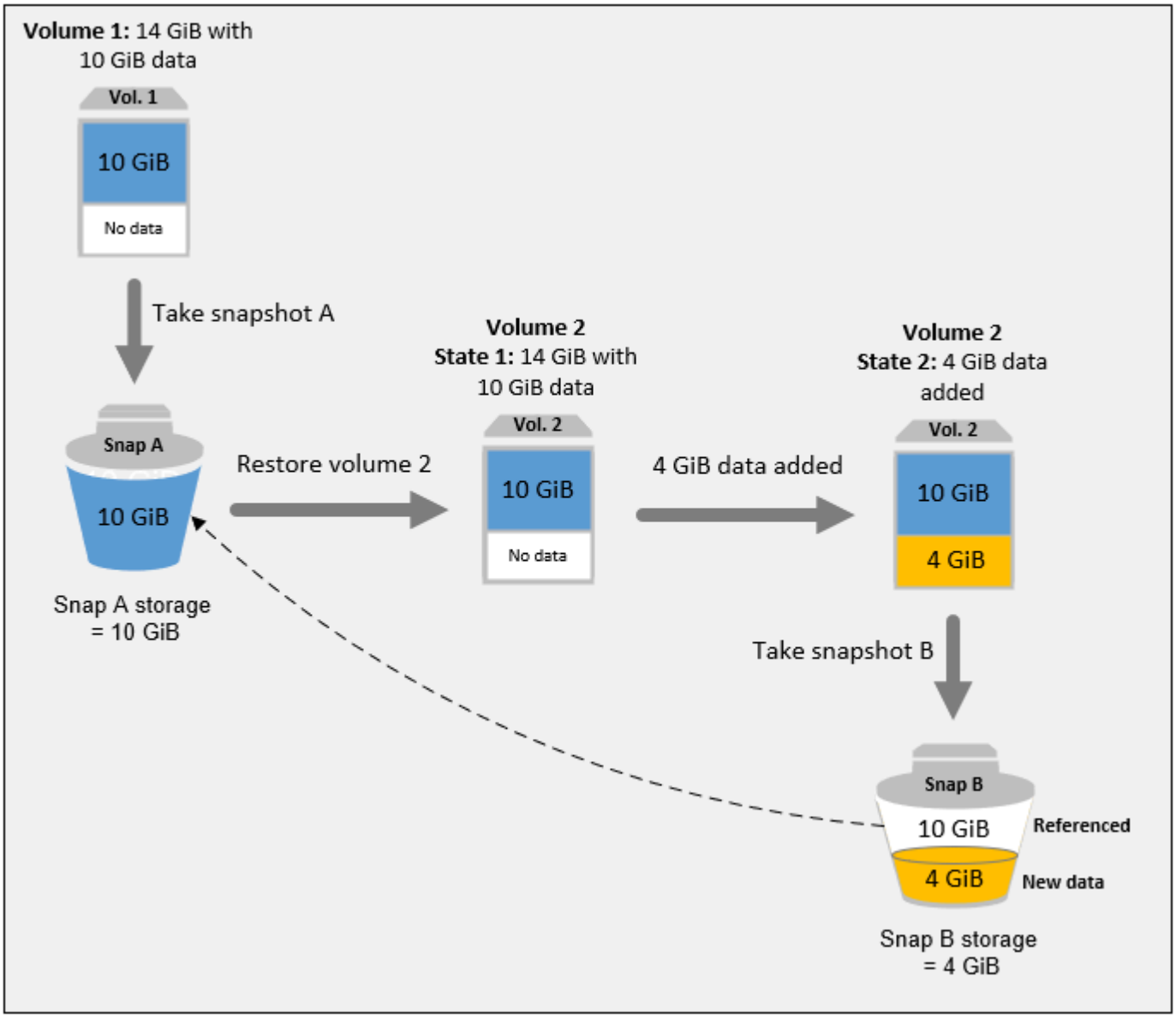
Snapshots incrementais de diferentes volumes

O diagrama nesta seção mostra como snapshots incrementais podem ser obtidos de diferentes volumes.

1. Vol 1, que tem `14 GiB` de tamanho, tem `10 GiB` de dados. Como Snap A é o primeiro snapshot criado do volume, ele é um snapshot completo e todos os `10 GiB` de dados são copiados e armazenados em backup.
2. O Vol 2 é criado do Snap A, por isso é uma réplica exata do Vol 1 no momento em que o snapshot foi criado.
3. Ao longo do tempo, `4 GiB` de dados são adicionados ao Vol 2 e seu tamanho total dos seus dados é `14 GiB`.
4. O Snap B é criado do Vol 2. Para o Snap B, apenas os `4 GiB` de dados adicionados depois que o volume foi criado a partir do Snap A são copiados e armazenados. Os outros `10 GiB` de dados inalterados, que já estão armazenados no Snap A, são referenciados pelo Snap B em vez de ser feito backup novamente.

   O Snap B é um snapshot incremental do Snap A, mesmo que tenha sido criado de um volume diferente.

> **Important**
>
> O diagrama pressupõe que você possui o Vol 1 e o Snap A, e que o Vol 2 está criptografado com a mesma chave KMS que o Vol 1. Se o Vol 1 pertencesse a outra AWS conta e essa conta pegasse o Snap A e o compartilhasse com você, o Snap B seria um instantâneo completo. Ou, se o Vol 2 fosse criptografado com uma chave KMS diferente do Vol 1, o Snap B seria um snapshot completo.



Para obter mais informações sobre como os dados são gerenciados ao excluir um snapshot, consulte Excluir um snapshot do Amazon EBS.

Copiar e compartilhar snapshots

Você pode compartilhar um instantâneo entre AWS contas modificando suas permissões de acesso. É possível fazer cópias de seus próprios snapshots e também de snapshots que foram compartilhados com você. Para ter mais informações, consulte Compartilhar um snapshot do Amazon EBS.

Um instantâneo é restrito à AWS região em que foi criado. Após criar um snapshot de um volume do EBS, é possível usá-lo para criar novos volumes na mesma região. Para obter mais informações, consulte Criar um volume a partir de um snapshot. Também é possível copiar os snapshots entre regiões, possibilitando o uso de múltiplas regiões para expansão geográfica, migração de datacenters e recuperação de desastres. É possível copiar qualquer snapshot acessível que tenha um status de `completed`. Para obter mais informações, consulte Copiar um snapshot do Amazon EBS..

Suporte a criptografia para snapshots

Os snapshots do EBS oferecem suporte completo à criptografia do EBS.

- Snapshots de volumes criptografados são criptografados automaticamente.
- Os volumes criados a partir de snapshots criptografados são criptografados automaticamente.
- Os volumes que você cria a partir de um snapshot não criptografado que você possui ou ao qual tem acesso podem ser criptografados. on-the-fly
- Quando você copia um snapshot não criptografado que você possua, pode criptografá-lo durante o processo de cópia.
- Quando você copia um snapshot criptografado que você possua ou ao qual tenha acesso, pode recriptografá-lo com uma chave diferente durante o processo de cópia.
- O primeiro snapshot que você fizer de um volume criptografado criado a partir de um snapshot não criptografado sempre será um snapshot completo.
- O primeiro snapshot que você fizer de um volume recriptografado, que tem um CMK diferente em relação ao snapshot de origem, sempre será um snapshot completo.

A documentação completa de cenários possíveis de criptografia do snapshot é fornecida em Criar snapshots de Amazon EBS e em Copiar um snapshot do Amazon EBS..

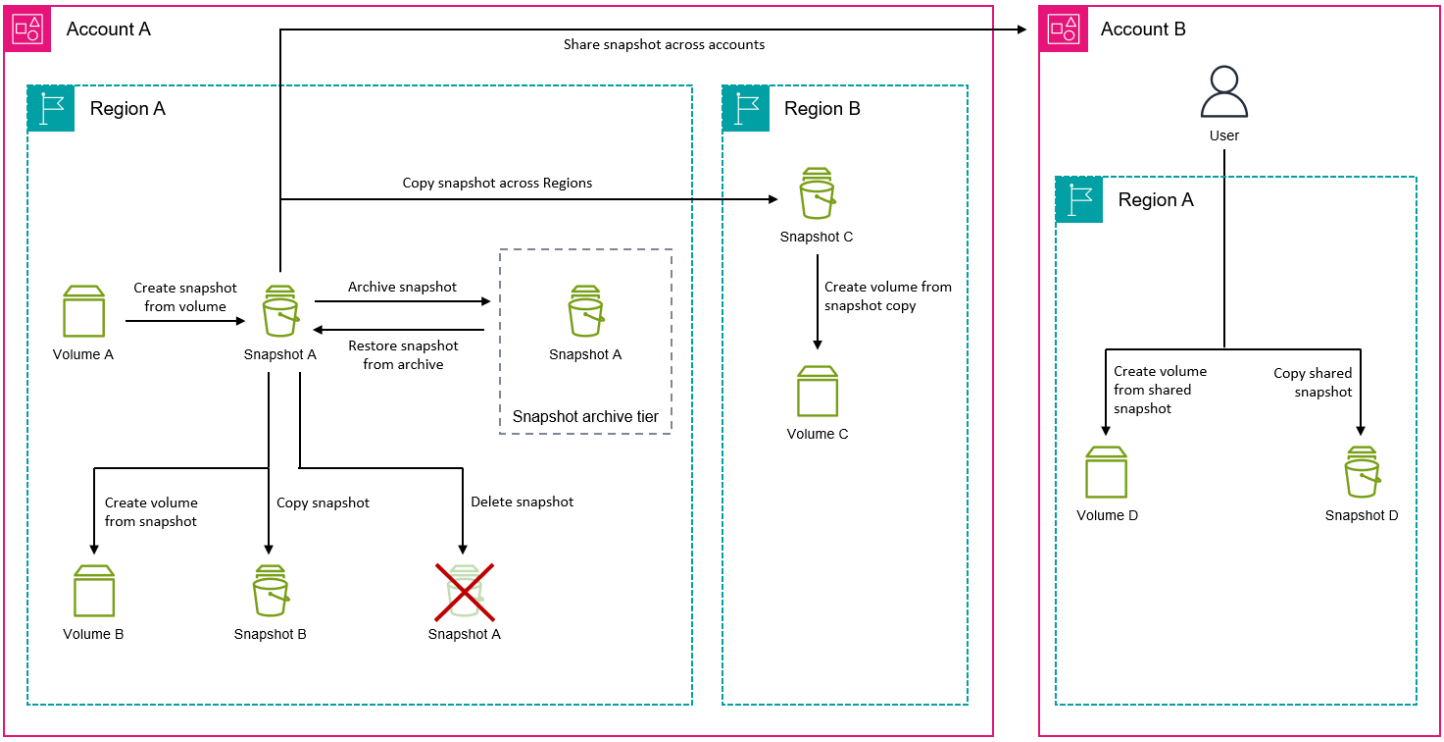
Para ter mais informações, consulte Criptografia do Amazon EBS.

Ciclo de vida do snapshot do Amazon EBS

O ciclo de vida de um snapshot do Amazon EBS começa com o processo de criação. Os snapshots são criados dos volumes do Amazon EBS. Eles podem ser usados para restaurar novos volumes do Amazon EBS. É possível criar cópias de snapshots na mesma região ou em regiões diferentes. Você pode compartilhar instantâneos com outras pessoas Contas da AWS, seja de forma pública ou

privada. Essas contas podem restaurar volumes com base nos snapshots compartilhados ou podem criar cópias dos snapshots compartilhados em suas próprias contas. Se você não precisar de acesso imediato a um snapshot, poderá arquivá-lo para economizar gastos com armazenamento.

A imagem a seguir mostra as ações que podem ser realizadas em seus snapshots como parte do ciclo de vida do snapshot.



Tarefas

- Criar snapshots de Amazon EBS
- Exibir informações do snapshot do Amazon EBS
- Copiar um snapshot do Amazon EBS.
- Compartilhar um snapshot do Amazon EBS
- Arquivar snapshots do Amazon EBS
- Excluir um snapshot do Amazon EBS
- Automatizar o ciclo de vida do snapshot

Criar snapshots de Amazon EBS

Para criar snapshots consistentes com aplicações em uma instância do Windows, consulte Criar um snapshot consistente com aplicações do VSS.

Você pode criar um point-in-time snapshot de um volume do EBS e usá-lo como linha de base para novos volumes ou para backup de dados. Se você fizer snapshots periódicos de um volume, eles serão incrementais — o novo snapshot salvará somente os blocos alterados desde o último snapshot.

Os snapshots ocorrem de forma assíncrona; o point-in-time snapshot é criado imediatamente, mas o status do snapshot é `pending` até que o snapshot seja concluído (quando todos os blocos modificados tiverem sido transferidos para o Amazon S3), o que pode levar várias horas para snapshots iniciais grandes ou instantâneos subsequentes em que muitos blocos foram alterados. Enquanto está sendo concluído, um snapshot em andamento não é afetado pelas leituras e gravações contínuas do volume.

É possível tirar um snapshot de um volume anexado que esteja em uso. No entanto, os snapshots só capturam dados gravados no seu volume do Amazon EBS no momento em que o comando do snapshot é emitido. Isso pode excluir quaisquer dados em cache por quaisquer aplicações ou sistemas operacionais. Se você puder pausar a gravação de qualquer arquivo para o volume por tempo suficiente para tirar um snapshot, seu snapshot deverá estar completo. Contudo, se você não puder pausar todas as gravações do arquivo para o volume, deve desmontar o volume de dentro da instância, emitir o comando de snapshot e remontar o volume para garantir um snapshot consistente e completo. É possível remontar e usar o volume enquanto o status do snapshot for `pending`.

Para facilitar o gerenciamento de snapshots, é possível marcar os snapshots durante a criação ou adicionar tags posteriormente. Por exemplo, é possível aplicar tags que descrevem o volume original a partir do qual o snapshot foi criado ou o nome do dispositivo usado para associar o volume original a uma instância.

Criptografia de snapshot

Os snapshots tirados dos volumes criptografados são criptografados automaticamente. Os volumes criados a partir de snapshots criptografados também são criptografados automaticamente. Os dados nos seus volumes criptografados e em quaisquer snapshots associados estão protegidos em repouso e em movimento. Para ter mais informações, consulte Criptografia do Amazon EBS.

Por padrão, só é possível criar volumes a partir dos snapshots que possui. No entanto, você pode compartilhar seus instantâneos não criptografados com AWS contas específicas ou pode compartilhá-los com toda a AWS comunidade, tornando-os públicos. Para ter mais informações, consulte Compartilhar um snapshot do Amazon EBS.

Você pode compartilhar um instantâneo criptografado somente com AWS contas específicas. Para que outros usem o snapshot compartilhado e criptografado, é preciso também compartilhar

a chave CMK usada para criptografá-lo. Os usuários com acesso ao seu snapshot criptografado devem criar sua própria cópia pessoal e usar essa cópia. Sua cópia de um snapshot compartilhado e criptografado também pode ser recriptografada usando uma chave diferente. Para obter mais informações, consulte Compartilhar um snapshot do Amazon EBS.

Snapshots de vários volumes

Você pode criar instantâneos de vários volumes, que são point-in-time instantâneos de todos ou alguns dos volumes anexados a uma instância.

Por padrão, quando você cria snapshots de vários volumes com base em uma instância, o Amazon EBS cria snapshots de todos os volumes (raiz e dados [não raiz]) que estão anexados à instância. Porém, você pode optar por criar snapshots de um subconjunto dos volumes anexados à instância.

É possível marcar os snapshots de vários volumes como você faria com um único snapshot de volume. Recomendamos marcar os snapshots de vários volumes para gerenciá-los coletivamente durante a restauração, cópia ou retenção. Também é possível optar por copiar automaticamente as tags do volume de origem nos snapshots correspondentes. Isso ajuda a definir os metadados do snapshot, como políticas de acesso, informações de anexo e alocação de custos, de acordo com o volume de origem.

Depois que os snapshots são criados, cada snapshot é tratado como um snapshot individual. É possível realizar todas as operações de snapshot, como restaurar, excluir e copiar entre regiões ou contas, assim como o faria com um único snapshot de volume.

Os snapshots de vários volumes e consistentes com falhas normalmente são restaurados como um conjunto. Isso é útil para identificar os snapshots que estão em um conjunto consistente com falhas marcando seu conjunto com o ID da instância, o nome ou outros detalhes relevantes.

Depois de criar seus snapshots, eles aparecem exatamente no console do EC2 criado. point-in-time

Se algum instantâneo do conjunto de instantâneos de vários volumes falhar, todos os outros instantâneos exibirão um status de erro e um `createSnapshots` CloudWatch evento com o resultado de será enviado para sua `failed` conta. AWS Para ter mais informações, consulte Criar snapshots (createSnapshots).

Amazon Data Lifecycle Manager

É possível criar políticas de ciclo de vida de snapshot para automatizar a criação e a retenção de snapshots de volumes individuais e de snapshots de vários volumes de instâncias. Para ter mais informações, consulte Amazon Data Lifecycle Manager.

Considerações

As seguintes considerações se aplicam à criação de snapshots:

- Para criar um snapshot para um volume do EBS que sirva como dispositivo raiz, recomendamos que você interrompa a instância antes de fazer o snapshot.
- Não é possível criar snapshots de instâncias para as quais a hibernação está habilitada ou de instâncias hibernadas. Se você criar um snapshot ou uma AMI com base em uma instância que está hibernada ou que tenha hibernação habilitada, talvez não consiga se conectar a uma nova instância iniciada da AMI ou de uma AMI criada pelo snapshot.
- Embora você possa tirar um snapshot de um volume enquanto um snapshot anterior desse volume esteja no status `pending`, ter vários snapshots `pending` de um volume pode resultar em performance reduzida do volume até que o snapshot seja concluído.
- Há um limite de um snapshot `pending` para um único volume de `st1` ou `desc1`, ou cinco snapshots `pending` para um único volume dos outros tipos de volume. Se você receber um erro `ConcurrentSnapshotLimitExceeded` ao tentar criar vários snapshots simultâneos do mesmo volume, aguarde até que um ou mais snapshots `pending` sejam concluídos antes de criar outro snapshot desse volume.
- Quando um instantâneo é criado a partir de um volume com um código de AWS Marketplace produto, o código do produto é propagado para o instantâneo.
- Ao criar conjuntos de snapshots de vários volumes com base em instâncias, é possível especificar até 127 volumes de dados (não raiz) a serem excluídos. O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Para obter mais informações, consulte Limites de volume por instância.

Criar um snapshot

Para criar um snapshot do volume especificado, use um dos métodos a seguir.

Console

Para criar um snapshot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Snapshots e Public Snapshots (Snapshots públicos).
3. Em Tipo de recurso, selecione Volume.

4. Em Volume ID (ID do volume) selecione o snapshot a partir do qual o volume será criado.

   O campo Encryption (Criptografia) indica o status de criptografia do volume selecionado. Se o volume selecionado for criptografado, o snapshot será criptografado automaticamente usando a mesma chave do KMS. Se o volume selecionado não for criptografado, o snapshot não será criptografado.
5. (Opcional) Em Description (Descrição), insira uma breve descrição para o snapshot.
6. (Opcional) Para atribuir tags personalizadas ao snapshot, na seção Tags, escolha Add tag (Adicionar tag) e insira o par chave-valor. É possível adicionar até 50 tags.
7. Escolha Criar snapshot.

AWS CLI

Para criar um instantâneo usando o AWS CLI

Use o comando create-snapshot (Criar snapshot).

Tools for Windows PowerShell

Para criar um instantâneo usando as Ferramentas para Windows PowerShell

Use o comando New-EC2Snapshot.

Criar um snapshot de vários volumes

Ao criar um conjunto de snapshots de vários volumes com base em uma instância, você pode escolher se deseja copiar as etiquetas do volume de origem para o snapshot correspondente. Você pode especificar se criará ou não um snapshot do volume raiz. Também é possível especificar se deseja criar snapshots de todos os volumes de dados (não raiz) anexados à instância ou se deseja criar snapshots de um subconjunto desses volumes.

Considerações

- Os snapshots de vários volumes oferecem suporte a até 128 volumes do Amazon EBS para cada instância, o que inclui o volume raiz e até 127 volumes de dados (não raiz). O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Para obter mais informações, consulte Limites de volume por instância.

Para criar um snapshot dos volumes de uma instância, use um dos métodos a seguir.

Console

Para criar snapshots de vários volumes usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Snapshots e Public Snapshots (Snapshots públicos).
3. Em Resource type (Tipo de recurso), escolha Instance (Instância).
4. Em Description (Descrição), insira uma breve descrição dos snapshots. Essa descrição é aplicada a todos os snapshots.
5. (Opcional) Por padrão, o Amazon EBS cria um snapshot do volume raiz da instância. Se não quiser criar um snapshot do volume raiz da instância, selecione Exclude root volume (Excluir volume raiz).
6. (Opcional) Por padrão, o Amazon EBS cria snapshots de todos os volumes de dados (não raiz) anexados à instância. Para criar snapshots de um subconjunto dos volumes de dados (não raiz) anexados à instância, selecione Exclude specific data volumes (Excluir volumes de dados específicos). A seção Attached data volumes (Volumes de dados anexados) lista todos os volumes de dados que atualmente estão anexados à instância selecionada.

   Na seção Attached data volumes (Volumes de dados anexados), selecione os volumes de dados para os quais você não quer criar snapshots. Somente os volumes que não forem selecionados serão incluídos no conjunto de snapshots de vários volumes. É possível excluir até 127 volumes.
7. (Opcional) Para copiar automaticamente as etiquetas dos volumes de origem para os snapshots correspondentes, para Copy tags from source volume (Copiar etiquetas do volume de origem), selecione Copy tags (Copiar etiquetas). Isso define os metadados do snapshot, como políticas de acesso, informações de anexo e alocação de custos, para corresponderem com o volume de origem.
8. (Opcional) Para atribuir outras etiquetas personalizadas a snapshots, na seção Tags (Etiquetas), escolha Add tag (Adicionar etiqueta) e insira o par chave-valor. É possível adicionar até 50 tags.
9. Escolha Criar snapshot.

   Durante a criação do snapshot, os snapshots são gerenciados juntos. Se houver falha em um dos snapshots do conjunto de volume, os outros snapshots serão movidos para o status de erro do conjunto de volume. Você pode monitorar o progresso dos seus instantâneos usando CloudWatchEventos. Após a conclusão do processo de criação do instantâneo, CloudWatch

gera um evento que contém o status e todos os detalhes relevantes do instantâneo para a instância afetada.

AWS CLI

Para criar instantâneos de vários volumes usando o AWS CLI, use o comando create-snapshots.

Caso não queira criar um snapshot do volume raiz, para `--instance-specification ExcludeBootVolume`, especifique `true`. Se não quiser criar snapshots de todos os volumes de dados (não raiz) anexados à instância, para `--instance-specification ExcludeDataVolumes`, especifique os IDs dos volumes de dados para os quais você não deseja criar snapshots. É possível especificar até 127 volumes de dados (não raiz) para exclusão.

Tools for Windows PowerShell;

Para criar instantâneos de vários volumes usando as Ferramentas para Windows PowerShell, use o New-EC2SnapshotBatchcomando.

Caso não queira criar um snapshot do volume raiz, para `-InstanceSpecification_ExcludeBootVolume`, especifique 1. Se não quiser criar snapshots de todos os volumes de dados (não raiz) anexados à instância, para `-InstanceSpecification_ExcludeDataVolumes`, especifique os IDs dos volumes de dados para os quais você não deseja criar snapshots. É possível especificar até 127 volumes de dados (não raiz) para exclusão.

Se todos os instantâneos forem concluídos com êxito, um `createSnapshots` CloudWatch evento com o resultado de `succeeded` será enviado para sua AWS conta. Se algum instantâneo do conjunto de instantâneos de vários volumes falhar, todos os outros instantâneos exibirão um status de erro e um `createSnapshots` CloudWatch evento com o resultado de será enviado para sua `failed` conta. AWS Para ter mais informações, consulte Criar snapshots (createSnapshots).

Como trabalhar com snapshots do EBS

É possível copiar snapshots, compartilhar snapshots e criar volumes de snapshots. Para mais informações, consulte:

- Copiar um snapshot do Amazon EBS.
- Compartilhar um snapshot do Amazon EBS

- Criar um volume a partir de um snapshot

Exibir informações do snapshot do Amazon EBS

É possível visualizar informações detalhadas sobre seus snapshots usando um dos métodos a seguir.

Console

Para visualizar informações de snapshots usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Para visualizar apenas os snapshots que pertencem a você, no canto superior esquerdo da tela, escolha Owned by me (Possuídos por mim). Também é possível filtrar seus snapshots usando tags e atributos de snapshot. No campo Filter (Filtro), selecione o campo de atributo e, em seguida, selecione ou insira o valor do atributo. Por exemplo, para visualizar apenas os snapshots criptografados, selecione Encryption (Criptografia) e insira `true`.
4. Para visualizar mais informações sobre um snapshot específico, escolha seu ID na lista.

AWS CLI

Para visualizar as informações do instantâneo usando o AWS CLI

Use o comando describe-snapshots.

Example Exemplo 1: filtro baseado em tags

O comando a seguir descreve os snapshots com a tag Stack=production.

```
aws ec2 describe-snapshots --filters Name=tag:Stack,Values=production
```

Example Exemplo 2: filtro baseado em volume

O comando a seguir descreve os snapshots criados do volume especificado.

```
aws ec2 describe-snapshots --filters Name=volume-id,Values=vol-049df61146c4d7901
```

Example Exemplo 3: filtro baseado na idade do snapshot

Com o AWS CLI, você pode usar o JMESPath para filtrar os resultados usando expressões. Por exemplo, o comando a seguir exibe os IDs de todos os snapshots criados pela sua conta da AWS (representada por *123456789012)* antes da data especificada (representada por *31/03/2020*). Se você não especificar o proprietário, os resultados incluirão todos os snapshots públicos.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

O comando a seguir exibe os IDs de todos os snapshots criados no intervalo de datas especificado.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]"
 --output text
```

Tools for Windows PowerShell

Para visualizar as informações do instantâneo usando as Ferramentas para Windows PowerShell

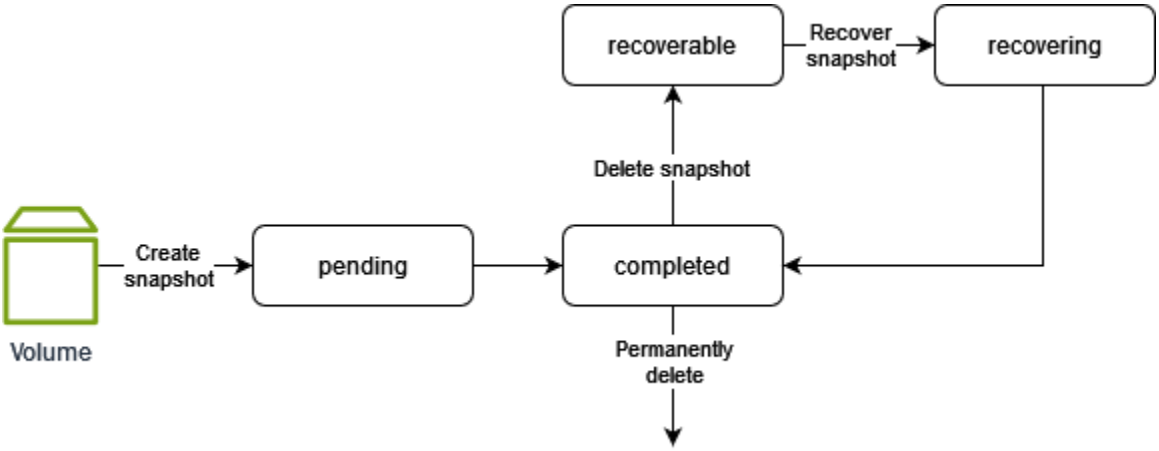
Use o comando Get-EC2Snapshot.

```
PS C:\> Get-EC2Snapshot -SnapshotId snapshot_id
```

Estados de um snapshot

Um snapshot do Amazon EBS passa por diferentes estados do momento em que é criado até sua exclusão permanente.

A ilustração a seguir mostra as transições entre estados de snapshots. Quando um snapshot é criado, ele entra no estado `pending`. Quando o snapshot estiver pronto para uso, ele entrará no estado `completed`. Ao perceber que não necessita mais de um snapshot, você poderá excluí-lo. Se você excluir um snapshot que corresponda a uma regra de retenção da Lixeira, ele será retido na Lixeira e entrará no estado `recoverable`. Se você recuperar um instantâneo da Lixeira, ele entrará no estado `recovering` e, em seguida, no estado `completed`. Caso contrário, ele será excluído permanentemente.



A tabela a seguir resume os estados dos snapshots.

Status	Descrição
`pending`	O processo de criação do snapshot ainda está em andamento. Um snapshot não pode ser usado enquanto está no estado `pending`.
`completed`	O processo de criação do snapshot foi concluído e ele está pronto para uso.
`recoverable`	O snapshot está na Lixeira. Para usar o snapshot, primeiro é necessário recuperá-lo da Lixeira.
`recovering`	O snapshot está sendo recuperado da Lixeira. Depois que o snapshot é recuperado, ele passa para o `completed` estado e se torna pronto para uso.
`error`	O processo de criação do snapshot falhou. Um snapshot não pode ser usado enquanto está no estado `error`.

Copiar um snapshot do Amazon EBS.

Com o Amazon EBS, você pode criar point-in-time snapshots de volumes, que armazenamos para você no Amazon S3. Depois de criar um snapshot e terminar de ser copiado para o Amazon S3 (quando o status do snapshot `completed` for), você poderá copiá-lo de AWS uma região para outra ou dentro da mesma região. A criptografia do lado do servidor do Amazon S3 (AES de 256 bits) protege os dados de um snapshot em trânsito durante uma operação de cópia. A cópia do snapshot recebe um ID diferente do ID do snapshot original.

Para copiar instantâneos de vários volumes para outra AWS região, recupere os instantâneos usando a tag que você aplicou ao conjunto de instantâneos de vários volumes ao criá-lo. Depois, copie cada snapshot para outra região.

Se você quiser que outra conta possa copiar seu instantâneo, você deve modificar as permissões do instantâneo para permitir o acesso a essa conta ou tornar o instantâneo público para que todas as AWS contas possam copiá-lo. Para ter mais informações, consulte Compartilhar um snapshot do Amazon EBS.

Para obter informações sobre como copiar um snapshot do Amazon RDS, consulte Cópia de um DB Snapshot no Guia do usuário da Amazon RDS.

Casos de uso

- Expansão geográfica: inicie seus aplicativos em uma nova AWS região.
- Migração: mova uma aplicação para uma nova região, de forma a permitir melhor disponibilidade e minimizar os custos.
- Recuperação de desastres: faça backup dos seus dados e logs em locais geográficos diferentes e intervalos regulares. Em caso de desastre, você pode restaurar seus aplicativos usando point-in-time backups armazenados na região secundária. Isso minimiza a perda de dados e o tempo de recuperação.
- Criptografia: criptografe um snapshot não criptografado previamente, altere a chave com a qual o snapshot foi criptografado ou crie uma cópia de sua propriedade para criar um volume a partir dela (para snapshots criptografados que foram compartilhados com você).
- Retenção de dados e requisitos de auditoria: copie seus snapshots do EBS criptografados de uma conta da AWS para outra para preservar os logs de dados ou outros arquivos para auditoria ou retenção de dados. Usar uma conta diferente ajuda a evitar exclusões acidentais de instantâneos e protege você se sua AWS conta principal for comprometida.

Conteúdos

Pré-requisitos

- É possível copiar todos os snapshots acessíveis que tenham o status `completed`, incluindo snapshots compartilhados e snapshots que você criou.
- Você pode copiar instantâneos AWS Marketplace, VM Import/Export e Storage Gateway, mas deve verificar se o instantâneo é suportado na região de destino.
- Para copiar um snapshot criptografado, o usuário deve ter as permissões para usar a criptografia do Amazon EBS a seguir.
  - `kms:DescribeKey`
  - `kms:CreateGrant`
  - `kms:GenerateDataKey`
  - `kms:GenerateDataKeyWithoutPlaintext`
  - `kms:ReEncrypt`
  - `kms:Decrypt`
- Para copiar um instantâneo criptografado compartilhado de outra AWS conta, você deve ter permissões para usar a chave gerenciada pelo cliente que foi usada para criptografar o instantâneo. Para ter mais informações, consulte Compartilhar uma chave do KMS.

Considerações

- Existe um limite de solicitações de cópia de `20` snapshots simultâneos por região de destino. Se você exceder essa cota, você receberá um erro `ResourceLimitExceeded`. Se você receber esse erro, aguarde até que uma ou mais solicitações de cópia sejam concluídas antes de fazer uma nova solicitação de cópia do snapshot.

- Tags definidas pelo usuário não são copiadas do snapshot de origem para o novo snapshot. É possível adicionar tags definidas pelo usuário durante ou depois da operação de cópia.
- Os snapshots criados por uma operação de cópia de snapshots têm um ID arbitrário de volume, como `vol-ffff` ou `vol-ffffffff`. Esses IDs arbitrários de volume não devem ser usados para qualquer outra finalidade.
- As permissões de nível de recurso especificadas para a operação de cópia de snapshot se aplicam somente ao novo snapshot. Você não pode especificar permissões no nível do recurso para o snapshot de origem. Para ver um exemplo, consulte Exemplo: copiar snapshots.

Definição de preço

- Para obter informações sobre preços sobre a cópia de snapshots entre AWS regiões e contas, consulte os preços do Amazon EBS.
- Se você copiar um snapshot e criptografá-lo com uma nova chave do KMS, será criada uma cópia completa (não incremental). Isso resulta em custos adicionais de armazenamento.
- Se você copiar um snapshot para uma nova região, uma cópia completa (não incremental) será criada. Isso resulta em custos adicionais de armazenamento. Cópias subsequentes do mesmo snapshot são incrementais.
- Se você usar transferências de dados externas ou entre regiões, cobranças adicionais de transferência de dados do EC2 serão aplicadas. Além disso, se você excluir algum snapshot após a inicialização, ainda receberá cobrança pelos dados que já foram transferidos.

Cópias incrementais de snapshots

A determinação de se uma cópia do snapshot deve ser incremental é feita pela cópia do snapshot concluída mais recentemente. Ao copiar um snapshot entre regiões ou contas, a cópia será uma cópia incremental se as seguintes condições forem atendidas:

- O snapshot foi copiado anteriormente na conta ou região de destino.
- A cópia mais recente do snapshot ainda existe na conta ou região de destino.
- A cópia instantânea mais recente não foi arquivada.
- Todas as cópias do snapshot na conta ou região de destino foram feitas sem criptografia ou foram criptografadas usando a mesma chave do KMS.

Se a cópia mais recente do snapshot tiver sido excluída, a próxima cópia será um cópia completa, não uma cópia incremental. Se uma cópia ainda estiver pendente quando outra cópia for iniciada, esta será iniciada somente após a primeira cópia ser concluída.

As operações de cópia instantânea na mesma conta e região usando a mesma chave KMS resultam em uma cópia incremental.

A cópia de snapshots incrementais reduz o tempo necessário para copiar snapshots e economiza em custos de transferência de dados e armazenamento por não duplicar os dados.

Recomendamos marcar seus snapshots com o ID do volume e a hora da criação para que você possa manter o controle da cópia do snapshot mais recente de um volume na conta ou região de destino.

Para ver se suas cópias de snapshot são incrementais, verifique o evento CopySnapshot. CloudWatch

Cópia de snapshot e criptografia

Quando você copiar um snapshot, poderá criptografar a cópia ou especificar uma chave do KMS diferente da original, e o snapshot copiado resultante usará a nova chave do KMS. Contudo, a alteração do status de criptografia de um snapshot durante uma operação de cópia pode resultar em uma cópia completa (não incremental), o que pode aumentar os custos de transferência e armazenamento de dados. Para ter mais informações, consulte Cópias incrementais de snapshots.

Para copiar um instantâneo criptografado compartilhado de outra AWS conta, você deve ter permissões para usar o instantâneo e a chave gerenciada pelo cliente (CMK) que foi usada para criptografar o instantâneo. Ao usar um snapshot criptografado que foi compartilhado com você, recomendamos que você refaça a criptografia do snapshot copiando-o por meio de uma chave do KMS própria. Isso protegerá você se a chave do KMS original estiver comprometida ou se o proprietário revogá-la, o que poderá fazer com que você perca o acesso aos volumes criptografados criados usando o snapshot. Para obter mais informações, consulte Compartilhar um snapshot do Amazon EBS.

Você aplica a criptografia a cópias de snapshots do EBS definindo o parâmetro `Encrypted` como `true`. (O parâmetro `Encrypted` é opcional se a opção encryption by default (criptografia por padrão) estiver ativada).

Opcionalmente, é possível usar `KmsKeyId` para especificar uma chave personalizada para criptografar a cópia do snapshot. (O parâmetro `Encrypted` também deve ser definido como

`true`, mesmo que a criptografia por padrão esteja ativada.) Se o parâmetro `KmsKeyId` não for especificado, a chave usada para a criptografia dependerá do estado de criptografia do snapshot de origem e de sua propriedade.

A tabela a seguir descreve os resultados da criptografia para cada combinação possível de configurações ao copiar snapshots que você possui e aos snapshots compartilhados com você.

Criptografia por padrão	O parâmetro **`Encrypted`** está definido?	Status de criptografia do snapshot de origem	Padrão (nenhuma chave do KMS especificada)	Personalizado (chave do KMS especificada)
Desabilitado	Não	Não criptografado	Não criptografado	N/D
		Criptografado	Criptografado por Chave gerenciada pela AWS	
	Sim	Não criptografado	Criptografado pela chave do KMS padrão	Criptografado pela chave do KMS especificada**
		Criptografado	Criptografado pela chave do KMS padrão	
Enabled	Não	Não criptografado	Criptografado pela chave do KMS padrão	N/D
		Criptografado	Criptografado pela chave do KMS padrão	
	Sim	Não criptografado	Criptografado pela chave do KMS padrão	Criptografado pela chave do

Criptografia por padrão	O parâmetro **`Encrypted`** está definido?	Status de criptografia do snapshot de origem	Padrão (nenhuma chave do KMS especificada)	Personalizado (chave do KMS especificada)
		Criptografado	Criptografado pela chave do KMS padrão	KMS especific ada**

** Essa é a chave do KMS especificada na ação de cópia do instantâneo. Essa chave do KMS é usada em vez da chave gerenciada pelo cliente padrão para a conta e a região.

Copiar um snapshot

Para copiar um snapshot, use um dos métodos a seguir.

Console

Para copiar um snapshot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot a ser copiado e escolha Actions (Ações), Copy snapshot (Copiar snapshot).
4. Em Description (Descrição), insira uma breve descrição do snapshot.

   Por padrão, a descrição inclui informações sobre o snapshot de origem, de forma que você possa diferenciar uma cópia do original. É possível alterar essa descrição conforme necessário.
5. Em Destination Region (Região de destino), selecione a região na qual criar a cópia do snapshot.
6. Especifique o status de criptografia da cópia do snapshot.

   Se o snapshot de origem for criptografado ou se sua conta for habilitada para criptografia por padrão, a criptografia será habilitada automaticamente e você não poderá desabilitá-la.

   Se o snapshot de origem não for criptografado e se sua conta não for habilitada para criptografia por padrão, a criptografia será opcional. Para criptografar a cópia do snapshot,

em Encryption (Criptografia), selecione Encrypt this snapshot (Criptografar este snapshot). Depois, para KMS key (Chave do KMS), selecione a chave do KMS a ser usada para criptografar o snapshot na região de destino.

7. Escolha Copy snapshot (Copiar snapshot).

AWS CLI

Para copiar um instantâneo usando o AWS CLI

Use o comando copy-snapshot (Copiar snapshot).

Tools for Windows PowerShell

Para copiar um instantâneo usando as Ferramentas para Windows PowerShell

Use o comando Copy-EC2Snapshot.

Para verificar se há falhas

Se você tentar copiar um snapshot criptografado sem ter permissão para usar a chave de criptografia, a operação falhará silenciosamente. O estado de erro não é exibido no console até você atualizar a página. Também é possível verificar o estado do snapshot a partir da linha de comando, conforme o exemplo a seguir.

```
aws ec2 describe-snapshots --snapshot-id snap-0123abcd
```

Se a cópia falhar devido a permissões de chave insuficientes, você verá a seguinte mensagem: "StateMessage“: “A ID da chave fornecida não está acessível”.

Para copiar um snapshot criptografado, é necessário ter as permissões `DescribeKey` no CMK padrão. Negar explicitamente essas permissões resulta em falha da cópia. Para obter mais informações sobre gerenciamento de chaves do CMK, consulte Autenticação e controle de acesso para o AWS KMS.

Compartilhar um snapshot do Amazon EBS

É possível modificar as permissões de um snapshot se você quiser compartilhá-lo com outras contas da AWS . Você pode compartilhar instantâneos publicamente com todas as outras AWS contas ou compartilhá-los de forma privada com AWS contas individuais que você especificar. Os usuários

autorizados podem usar os snapshots que você compartilhar para criar os próprios volumes do EBS, ao passo que seu snapshot original não será afetado.

> **Important**
>
> Ao compartilhar um snapshot, você está oferecendo a outras pessoas o acesso a todos os dados no snapshot. Compartilhe snapshots somente com as pessoas de sua confiança com todos os dados do snapshot.

Para evitar o compartilhamento público dos snapshots, você pode habilitar o bloqueio do acesso público aos snapshots. Para obter mais informações, consulte Bloquear o acesso público a suas AMIs.

Tópicos

Antes de compartilhar um snapshot

As seguintes considerações se aplicam ao compartilhamento de snapshots:

- Se o bloqueio do acesso público aos snapshots estiver habilitado para a região, tentativas de compartilhar publicamente os snapshots serão bloqueadas. Os snapshots ainda podem ser compartilhados de modo privado.
- Os snapshots são restritos à região na qual foram criados. Para compartilhar um snapshot com outra região, copie o snapshot nessa região e, em seguida, compartilhe a cópia. Para ter mais informações, consulte Copiar um snapshot do Amazon EBS..
- Não é possível compartilhar snapshots criptografados com a Chave gerenciada pela AWS padrão. Você só pode compartilhar snapshots criptografados com uma chave gerenciada pelo cliente. Para obter mais informações, consulte Criação de chaves no Guia do desenvolvedor AWS Key Management Service .

- É possível compartilhar apenas snapshots não criptografados publicamente.
- Ao compartilhar um snapshot criptografado, também é necessário compartilhar a chave gerenciada pelo cliente usada para criptografar o snapshot. Para obter mais informações, consulte Compartilhar uma chave do KMS.

Compartilhar um snapshot

É possível compartilhar um snapshot usando um dos métodos descritos na seção.

Console

Para compartilhar um snapshot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot a ser compartilhado e escolha Actions (Ações), Modify Permissions (Modificar permissões).
4. Especifique as permissões do snapshot. A Current setting (Configuração atual) indica as permissões atuais de compartilhamento do snapshot.
   - Para compartilhar o instantâneo publicamente com todas as AWS contas, escolha Público.
   - Para compartilhar o instantâneo de forma privada com AWS contas específicas, escolha Privado. Na seção Sharing accounts (Contas de compartilhamento), selecione Add account (Adicionar conta) e insira o ID de 12 dígitos (sem hifens) da conta com a qual compartilhar.
5. Escolha Salvar alterações.

AWS CLI

As permissões de um snapshot são especificadas usando o atributo `createVolumePermission` do snapshot. Para tornar um snapshot público, defina o grupo como `all`. Para compartilhar um instantâneo com uma AWS conta específica, defina o usuário como o ID da AWS conta.

Para compartilhar um snapshot publicamente

Use o comando modify-snapshot-attribute.

Para `--attribute`, especifique `createVolumePermission`. Para `--operation-type`, especifique `add`. Para `--group-names`, especifique `all`.

```
$  aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute
 createVolumePermission --operation-type add --group-names all
```

Para compartilhar um snapshot de forma privada

Use o comando modify-snapshot-attribute.

Para `--attribute`, especifique `createVolumePermission`. Para `--operation-type`, especifique `add`. Para`--user-ids`, especifique os IDs de 12 dígitos das AWS contas com as quais compartilhar os instantâneos.

```
$  aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute
 createVolumePermission --operation-type add --user-ids 123456789012
```

Tools for Windows PowerShell

As permissões de um snapshot são especificadas usando o atributo `createVolumePermission` do snapshot. Para tornar um snapshot público, defina o grupo como `all`. Para compartilhar um instantâneo com uma AWS conta específica, defina o usuário como o ID da AWS conta.

Para compartilhar um snapshot publicamente

Use o comando Edit-EC2SnapshotAttribute.

Para `-Attribute`, especifique `CreateVolumePermission`. Para `-OperationType`, especifique `Add`. Para `-GroupName`, especifique `all`.

```
PS C:\>  Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute
 CreateVolumePermission -OperationType Add -GroupName all
```

Para compartilhar um snapshot de forma privada

Use o comando Edit-EC2SnapshotAttribute.

Para `-Attribute`, especifique `CreateVolumePermission`. Para `-OperationType`, especifique `Add`. Para`UserId`, especifique os IDs de 12 dígitos das AWS contas com as quais compartilhar os instantâneos.

```
PS C:\>  Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute
 CreateVolumePermission -OperationType Add -UserId 123456789012
```

Compartilhar uma chave do KMS

Ao compartilhar um snapshot criptografado, também é necessário compartilhar a chave gerenciada pelo cliente usada para criptografar o snapshot. É possível aplicar permissões entre contas a uma chave gerenciada pelo cliente quando ela é criada ou posteriormente.

Os usuários da sua chave gerenciada pelo cliente compartilhada que estão acessando snapshots criptografados devem receber permissões para executar as seguintes ações na chave:

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:GenerateDataKeyWithoutPlaintext`
- `kms:ReEncrypt`
- `kms:Decrypt`

> **Tip**
>
> Para seguir o princípio de menor privilégio, não permita acesso total a `kms:CreateGrant`. Em vez disso, use a chave de `kms:GrantIsForAWSResource` condição para permitir que o usuário crie concessões na chave KMS somente quando a concessão for criada em nome do usuário por um AWS serviço.

Para obter mais informações sobre como controlar o acesso a uma chave gerenciada pelo cliente, consulte Usar políticas de chaves no AWS KMS no Guia do desenvolvedor do AWS Key Management Service .

Para compartilhar a chave gerenciada pelo cliente usando o AWS KMS console

1. Abra o AWS KMS console em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.

3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Na coluna Alias, escolha o alias (link de texto) da chave gerenciada pelo cliente usada para criptografar o snapshot. Os principais detalhes são abertos em uma nova página.
5. Na seção Key policy (Política de chaves), você verá a exibição de política ou a exibição padrão. A exibição de política exibe o documento de política de chaves. A visualização padrão exibe seções para Administradores de chave, Exclusão de chave, Uso de chave e Outras contas da AWS . A exibição padrão é exibida se você criou a política no console e não a personalizou. Se a exibição padrão não estiver disponível, será necessário editar manualmente a política na exibição de política. Para obter mais informações, consulte Exibição de uma política de chaves (console) no Guia do desenvolvedor do AWS Key Management Service .

   Use a visualização da política ou a visualização padrão, dependendo da visualização que você pode acessar, para adicionar uma ou mais IDs de AWS conta à política, da seguinte forma:

   - (Exibição de política) Escolha Edit (Editar). Adicione uma ou mais IDs de AWS conta às seguintes declarações: `"Allow use of the key"` `"Allow attachment of persistent resources"` e. Escolha Salvar alterações. No exemplo a seguir, o ID da AWS conta `444455556666` é adicionado à política.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
```

```
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

- (Visualização padrão) Role para baixo até Outras AWS contas. Escolha Adicionar outras AWS contas e insira o ID da AWS conta conforme solicitado. Para adicionar outra conta, escolha Adicionar outra AWS conta e insira o ID da AWS conta. Depois de adicionar todas as contas da AWS , escolha Save changes (Salvar alterações).

Exibir snapshots que são compartilhados com você

Use um dos métodos a seguir para visualizar snapshots compartilhados com você.

Console

Para visualizar snapshots compartilhados usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Filtre os instantâneos listados. No canto superior esquerdo da tela, escolha uma das seguintes opções:
   - Snapshots privados: para visualizar somente snapshots compartilhados com você de forma privada.
   - Snapshots públicos: para visualizar somente snapshots compartilhados com você publicamente.

AWS CLI

Para visualizar permissões de snapshots usando a linha de comando

Use o comando describe-snapshot-attribute.

Tools for Windows PowerShell

Para visualizar permissões de snapshots usando a linha de comando

Use o comando Get-EC2SnapshotAttribute.

Usar snapshots que são compartilhados com você

Para usar um snapshot compartilhado não criptografado

Localize o snapshot compartilhado pelo ID ou pela descrição. Para obter mais informações, consulte Exibir snapshots que são compartilhados com você. É possível usar esse instantâneo como faria com qualquer outro snapshot que você tenha na sua conta. Por exemplo, é possível criar um volume do snapshot ou copiá-lo para outra região.

Para usar um snapshot criptografado compartilhado

Localize o snapshot compartilhado pelo ID ou pela descrição. Para obter mais informações, consulte Exibir snapshots que são compartilhados com você. Crie uma cópia do snapshot compartilhado em sua conta e criptografe-a com uma chave do KMS de sua propriedade. Em seguida, é possível usar a cópia para criar volumes ou copiá-la para regiões diferentes.

Determinar o uso de snapshots compartilhados por você

Você pode usar AWS CloudTrail para monitorar se um instantâneo que você compartilhou com outras pessoas foi copiado ou usado para criar um volume. Os seguintes eventos estão registrados: CloudTrail

- SharedSnapshotCopyInitiated— Um instantâneo compartilhado está sendo copiado.
- SharedSnapshotVolumeCreated— Um instantâneo compartilhado está sendo usado para criar um volume.

Para obter mais informações sobre o uso CloudTrail, consulte Registrar chamadas de API do Amazon EC2 e do Amazon EBS com. AWS CloudTrail

Arquivar snapshots do Amazon EBS

O Arquivo de Snapshots do Amazon EBS é um novo nível de armazenamento que é possível usar para armazenamento de baixo custo e longo prazo dos snapshots que não requerem recuperação frequente ou rápida.

Por padrão, quando você cria um snapshot, ele é armazenado na camada padrão para snapshots do Amazon EBS (camada padrão). Os snapshots armazenados na camada padrão são incrementais. Isso significa que apenas os blocos de volumes que foram alterados após o snapshot mais recente são salvos.

Quando você arquiva um snapshot, o snapshot incremental é convertido em um snapshot completo e é movido da camada padrão para a camada de arquivo de snapshots do Amazon EBS (camada de arquivo). Os snapshots completos incluem todos os blocos que foram gravados no volume no momento em que o snapshot foi criado.

Quando você precisa acessar um snapshot arquivado, pode restaurá-lo da camada de arquivo para a camada padrão e usá-lo como usa qualquer outro snapshot em sua conta.

O Arquivo de Snapshots do Amazon EBS oferece custos de armazenamento de snapshots até 75% menores para os snapshots que você planeja armazenar por 90 dias ou mais e que não precisa acessar com frequência.

Alguns casos de uso típicos incluem:

- Arquivar o único snapshot de um volume, como snapshots de fim de projeto
- Arquivar snapshots incrementais completos de um momento específico por motivos de conformidade.
- Arquivar snapshots incrementais mensais, trimestrais ou anuais.

Tópicos

Considerações e limitações

Considerações

- O período de arquivamento mínimo é de 90 dias. Se você excluir ou restaurar permanentemente um snapshot arquivado antes do período mínimo de arquivamento de 90 dias, os dias restantes na camada de arquivo serão cobrados, arredondados para a hora mais próxima. Para obter mais informações, consulte Definição de preço e faturamento.
- Pode levar até 72 horas para restaurar um snapshot arquivado da camada de arquivo para a camada padrão, dependendo do tamanho do snapshot.
- Os snapshots arquivados são sempre snapshots completos. Um snapshot completo inclui todos os blocos que foram gravados no volume no momento em que o snapshot foi criado. O snapshot completo provavelmente será maior do que o snapshot incremental do qual ele foi criado. No entanto, se você tiver apenas um snapshot incremental de um volume na camada padrão, o tamanho do snapshot completo na camada de arquivo será igual ao tamanho do snapshot na camada padrão. Isso ocorre porque o primeiro snapshot feito de um volume é sempre um snapshot completo.
- O arquivamento é recomendado para snapshots mensais, trimestrais ou anuais. O arquivamento de snapshots incrementais diários de um único volume pode gerar custos mais altos em comparação com a manutenção deles no nível padrão.
- Quando um snapshot é arquivado, os dados referenciados por outros snapshots na linhagem dele são retidos na camada padrão. Os custos de dados e armazenamento associados aos dados referenciados retidos na camada padrão são alocados para o próximo snapshot na linhagem. Isso garante que os snapshots subsequentes na linhagem não sejam afetados pelo arquivamento.
- Se você excluir um snapshot arquivado que corresponda a uma regra de retenção da lixeira, o snapshot arquivado será retido na lixeira pelo período de retenção definido na regra. Para usar o snapshot, primeiro é necessário recuperá-lo da lixeira e depois restaurá-lo da camada de arquivo. Para obter mais informações, consulte Lixeira e Definição de preço e faturamento.
- Você não pode usar um snapshot arquivado em um mapeamento de dispositivos de blocos nem para criar um volume do Amazon EBS.
- Você pode arquivar os snapshots criados pelo AWS Backup usando o Console do AWS Backup, APIs ou ferramentas de linha de comando. Para obter mais informações, consulte Creating a backup plan no AWS Backup Developer Guide.

Limitações

- Você só pode arquivar snapshots que estejam no estado `completed`.
- Só é possível arquivar os snapshots que você possui na sua conta. Para arquivar um snapshot compartilhado com você, primeiro copie o snapshot para sua conta e depois arquive a cópia do snapshot.
- Antes de poder usar um snapshot arquivado, é necessário restaurá-lo para a camada padrão. A restauração ao nível padrão é necessária para criar um volume com base no snapshot por meio das operações `CreateVolume` e `RunInstances` da API, bem como para compartilhar ou copiar um snapshot. Para obter mais informações, consulte Restaurar um snapshot arquivado.
- Você poderá arquivar um snapshot associado a uma ou mais AMIs somente se todas as AMIs associadas estiverem desabilitadas. Para obter mais informações, consulte Desabilitar uma AMI.
- Você não poderá habilitar uma AMI desabilitada se os snapshots associados forem restaurados temporariamente. Todos os snapshots associados devem ser restaurados permanentemente para que você consiga habilitar a AMI.
- Você não pode cancelar o processo de arquivamento de snapshots nem restaurar snapshots depois que o processo é iniciado.
- Não é possível compartilhar snapshots arquivados. Se você arquivar um snapshot compartilhado com outras contas, as contas com as quais o snapshot é compartilhado perderão o acesso após ele ser arquivado.
- Não é possível copiar snapshots arquivados. Se você precisar copiar um snapshot arquivado, primeiro deve restaurá-lo.
- Você não pode habilitar a restauração rápida de snapshots para um snapshot arquivado. A restauração rápida de snapshots é desabilitada automaticamente quando um snapshot é arquivado. Se precisar usar a restauração rápida de snapshots, você deverá habilitá-la manualmente após restaurá-lo.

Definição de preço e faturamento

Os snapshots arquivados são cobrados a uma taxa de USD 0,0125 por GB/mês. Por exemplo, se você arquivar um snapshot de 100 GiB, será cobrada uma taxa de USD 1,25 (100 GiB * USD 0,0125) por mês.

As restaurações de snapshots são cobradas a uma taxa de USD 0,03 por GB de dados restaurados. Por exemplo, se você restaurar um snapshot de 100 GiB da camada de arquivo, será cobrada uma taxa de USD 3 (100 GiB * USD 0,03).

Depois que o snapshot é restaurado para o nível padrão, ele é cobrado à taxa padrão para snapshots de USD 0,05 por GB/mês.

Para obter mais informações, consulte Definição de preço do Amazon EBS.

Faturamento pelo período mínimo de arquivamento

O período de arquivamento mínimo é de 90 dias. Se você excluir ou restaurar permanentemente um snapshot arquivado antes do período mínimo de arquivamento de 90 dias, será cobrada uma taxa pro-rata equivalente à taxa de armazenamento na camada de arquivo pelos dias restantes, arredondados para a hora mais próxima. Se, após 40 dias, você excluir ou restaurar permanentemente um snapshot arquivado, os 50 dias restantes do período mínimo de arquivamento serão cobrados.

> **Note**
>
> A restauração temporária de um snapshot arquivado antes do período mínimo de arquivamento de 90 dias não incorre nessa cobrança.

Restaurações temporárias

Quando você restaura temporariamente um snapshot, ele é restaurado da camada de arquivo para a camada padrão e uma cópia do snapshot permanece na camada de arquivo. Você recebe cobrança pelo snapshot na camada padrão e pela cópia do snapshot na camada de arquivo pela duração da restauração temporária. Quando o snapshot restaurado temporariamente é removido da camada padrão, você não receberá uma cobrança por ele, apenas pelo snapshot na camada de arquivo.

Restaurações permanentes

Quando você restaura permanentemente um snapshot, o snapshot é restaurado da camada de arquivo para a camada padrão, e é excluído da camada de arquivo. Você só recebe cobrança pelo snapshot na camada padrão.

Exclusão de snapshots

Se você excluir um snapshot enquanto ele estiver sendo arquivado, receberá cobrança pelos dados de snapshot que já tinham sido movidos para a camada de arquivo. Esses dados estão sujeitos

ao período mínimo de arquivamento de 90 dias e serão cobrados de acordo após a exclusão. Por exemplo, se você arquivar um snapshot de 100 GiB e excluir o snapshot após apenas 40 GiB terem sido arquivados, você receberá cobrança de USD 1,50 pelo período mínimo de arquivamento de 90 dias pelos 40 GiB já arquivados (USD 0,0125 por GB/mês * 40 GB * (90 dias * 24 horas) / (24 horas/dias * mês de 30 dias)).

Se você excluir um snapshot enquanto ele é restaurado da camada de arquivo, a restauração do snapshot será cobrada pelo tamanho total do snapshot (tamanho do snapshot * USD 0,03). Por exemplo, se você restaurar um snapshot de 100 GiB da camada de arquivo e excluir o snapshot a qualquer momento antes da conclusão da restauração do snapshot, será cobrada uma taxa de USD 3 (tamanho do snapshot de 100 GiB * USD 0,03).

lixeira

Os snapshots arquivados são cobrados conforme a taxa para snapshots arquivados enquanto estão na lixeira. Os snapshots arquivados que estão na lixeira estão sujeitos ao período mínimo de arquivamento de 90 dias e são cobrados de acordo se forem excluídos pela lixeira antes do período mínimo de arquivamento. Em outras palavras, se uma regra de retenção excluir um snapshot arquivado da lixeira antes do período mínimo de 90 dias, você receberá cobrança pelos dias restantes.

Se você excluir um snapshot que corresponda a uma regra de retenção enquanto ele estiver sendo arquivado, o snapshot arquivado será retido na lixeira pelo período de retenção definido na regra. Ele é cobrado conforme a taxa para snapshots arquivados.

Se você excluir um snapshot que corresponda a uma regra de retenção enquanto ele estiver sendo restaurado, o snapshot restaurado será retido na lixeira pelo resto do período de retenção e cobrado à taxa de snapshot padrão. Para usar o snapshot restaurado, primeiro é necessário recuperá-lo da lixeira.

Para obter mais informações, consulte Lixeira.

Controle de custos

Snapshots arquivados aparecem no AWS Cost and Usage Report com o mesmo ID de recurso e nome do recurso da Amazon (ARN). Para obter mais informações, consulte o AWS Cost and Usage ReportGuia do Usuário.

É possível usar os seguintes tipos de uso para identificar os custos associados:

- `SnapshotArchiveStorage`: taxa para armazenamento de dados mensal
- `SnapshotArchiveRetrieval`: taxa única para restaurações de snapshot
- `SnapshotArchiveEarlyDelete`: taxa para excluir ou restaurar permanentemente um snapshot antes do período mínimo de arquivamento (90 dias)

Cotas

Esta seção descreve as cotas padrão para snapshots arquivados e em andamento.

Cota	Cota padrão			
Snapshots arquivados por volume	25			
Arquivos de snapshots simultâneos em andamento por conta	25			
Resturações de snapshots simultâneos em andamento por conta	5			

Se você precisar de mais do que os limites padrão, preencha o formulário Create case do AWS Support Center para solicitar um aumento de limite.

Diretrizes e práticas recomendadas para arquivamento de snapshots

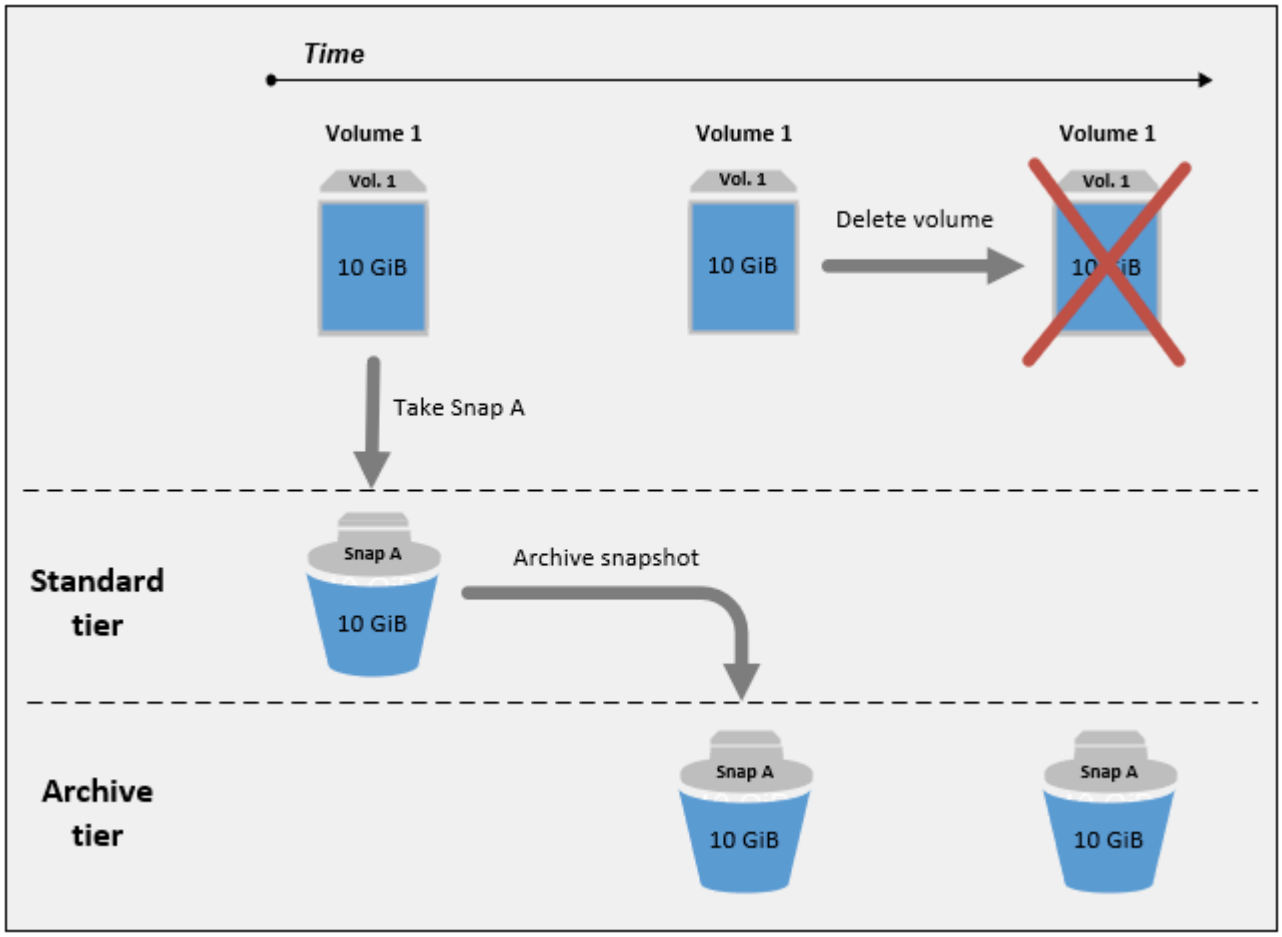
Esta seção oferece algumas diretrizes e práticas recomendadas para arquivamento de snapshots.

Tópicos

Arquivamento do único snapshot de um volume

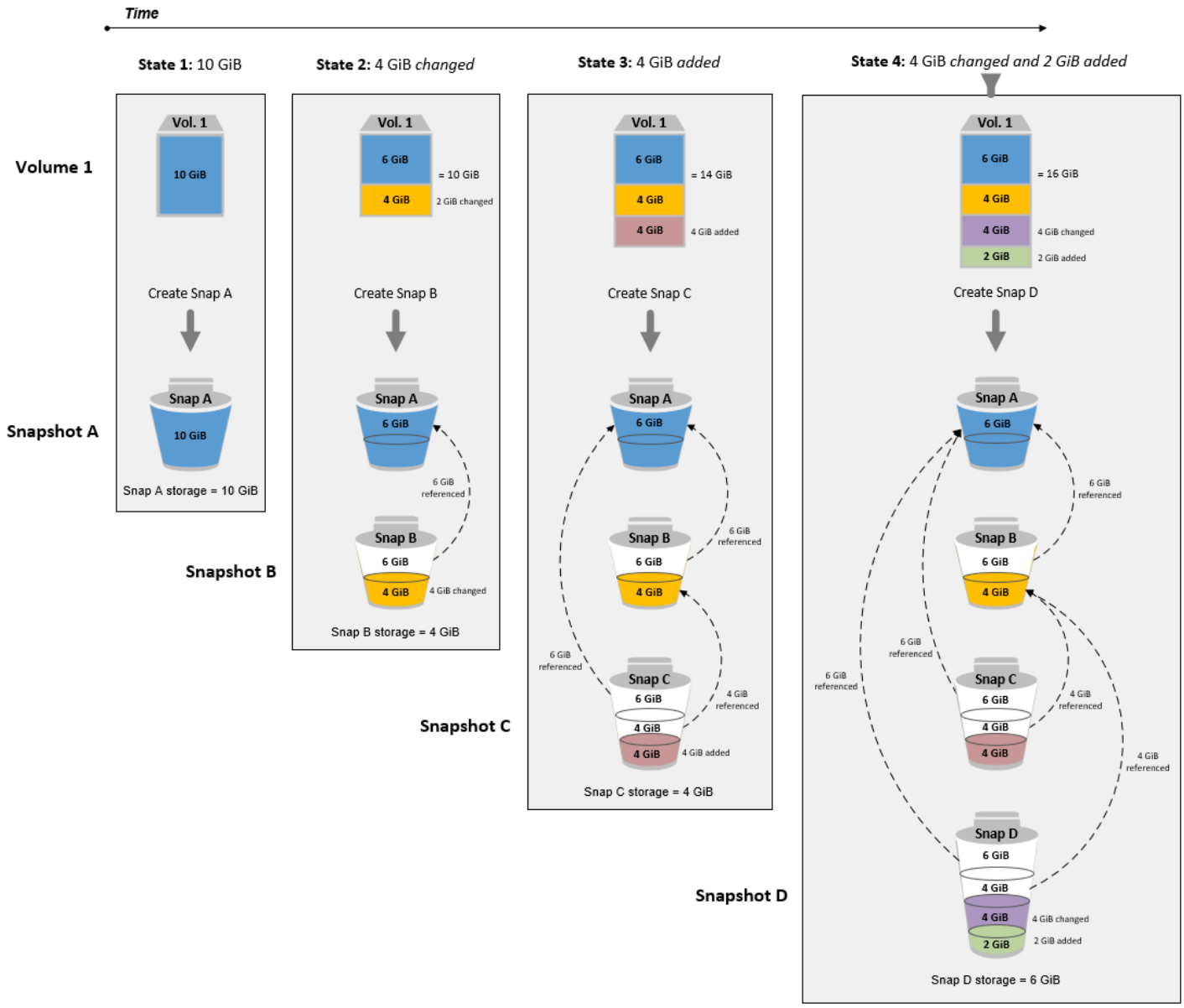
Quando você tem apenas um snapshot de um volume, o snapshot tem sempre o mesmo tamanho dos blocos gravados no volume no momento em que o snapshot foi criado. Quando você arquiva esse snapshot, o snapshot na camada padrão é convertido em um snapshot completo de tamanho equivalente e é movido da camada padrão para a camada de arquivo.

Arquivar esses snapshots pode ajudá-lo a economizar, com custos de armazenamento mais baixos. Se você não precisar mais do volume de origem, pode excluir o volume para economizar mais em custos de armazenamento.



Arquivamento de snapshots incrementais de um único volume

Quando você arquiva um snapshot incremental, ele é convertido em um snapshot completo e é movido para a camada de arquivo. Por exemplo, na imagem a seguir, se você arquivar Snap B, o snapshot é convertido em um snapshot completo de 10 GiB e movido para a camada de arquivo. Da mesma forma, se você arquivar o Snap C, o tamanho do snapshot completo na camada de arquivo é de 14 GiB.



Se estiver arquivando snapshots para reduzir os custos de armazenamento na camada padrão, você não deverá arquivar o primeiro snapshot em um conjunto de snapshots incrementais. Esses snapshots são referenciados por snapshots subsequentes na linhagem do snapshot. Na maioria dos casos, arquivar esses snapshots não reduzirá os custos de armazenamento.

> **Note**
>
> Você não deve arquivar o último snapshot de um conjunto de snapshots incrementais. O último snapshot é snapshot mais recente feito de um volume. Você precisará desse

snapshot na camada padrão se desejar criar volumes a partir dele no caso de um volume ser corrompido ou perdido.

Se você arquivar um snapshot com dados referenciados por um snapshot posterior na linhagem, os custos de armazenamento de dados e de armazenamento associados aos dados referenciados serão alocados para o snapshot posterior na linhagem. Nesse caso, arquivar os snapshots não reduzirá os custos armazenamento de dados e de armazenamento. Por exemplo, na imagem anterior, se você arquivar o Snap B, seus 4 GiB de dados serão atribuídos ao Snap C. Nesse caso, seus custos gerais de armazenamento aumentarão porque você incorrerá em custos de armazenamento para a versão completa do Snap B na camada de arquivo, e seus custos de armazenamento para a camada padrão permanecerão inalterados.

Se você arquivar o Snap C, o armazenamento da camada padrão diminuirá em 4 GiB porque os dados não são referenciados por nenhum outro snapshot posterior na linhagem. E o armazenamento da camada de arquivo aumentará em 14 GiB porque o snapshot será convertido em um snapshot completo.

Arquivamento de snapshots completos por motivos de conformidade

Pode ser necessário criar backups completos dos volumes mensal, trimestral ou anualmente por motivos de conformidade. Para esses backups, é possível precisar de snapshots autônomos sem referências retroativas ou avançadas a outros snapshots na linhagem dos snapshots. Os snapshots arquivados com o Arquivo de snapshots do EBS são snapshots completos e não têm nenhuma referência a outros snapshots na linhagem. Além disso, você provavelmente precisará reter esses snapshots por motivos de conformidade por vários anos. O Arquivo de snapshots do EBS torna econômico arquivar esses snapshots completos para retenção de longo prazo.

Determinar a redução nos custos de armazenamento do nível padrão

Se você desejar arquivar um snapshot incremental para reduzir os custos de armazenamento, considere o tamanho do snapshot completo na camada de arquivo e a redução no armazenamento no nível padrão. Esta seção explica como fazer isso.

Important

As respostas da API são precisas em termos de dados no ponto do tempo em que as APIs são chamadas. As respostas da API podem diferir à medida que os dados associados a um snapshot forem alterados em resultado de alterações na linhagem do snapshot.

Para determinar a redução de armazenamento e de custos de armazenamento no nível padrão, use as etapas a seguir.

1. Confira o tamanho do snapshot completo. Para determinar o tamanho do snapshot completo, use o comando list-snapshot-blocks. Em `--snapshot-id`, especifique o ID do snapshot que você deseja arquivar.

```
$  aws ebs list-snapshot-blocks --snapshot-id snapshot_id
```

Isso retorna informações sobre todos os blocos no snapshot especificado. O `BlockIndex` do último bloco retornado pelo comando indica o número de blocos no snapshot. O número de blocos multiplicado por 512 KiB, que é o tamanho do bloco de snapshot, fornece uma boa aproximação do tamanho do snapshot completo na camada de arquivo (blocos * 512 KiB = tamanho completo do snapshot).

Por exemplo, o comando a seguir lista os blocos do snapshot `snap-01234567890abcdef`.

```
$  aws ebs list-snapshot-blocks --snapshot-id snap-01234567890abcdef
```

A seguir está a saída do comando, com alguns blocos omitidos. A saída a seguir indica que o snapshot inclui cerca de 16.383 blocos de dados. Isso se aproxima de um tamanho do snapshot completo de cerca de 8 GiB (16.383 * 512 KiB = 7,99 GiB).

```
 {
    "VolumeSize": 8,
    "Blocks": [
        {
            "BlockToken": "ABgBAeShfa5RwG+RiWUg2pwmnCU/
YMnV7fGMxLbCWfEBEUmmuqac5RmoyVat",
            "BlockIndex": 0
        },
        {
            "BlockToken": "ABgBATdTONyThPUAbQhbUQXsn5TGoY/
J17GfE83j9WN7siupavOTw9E1KpFh",
            "BlockIndex": 1
        },
        {
            "BlockToken": "EBEUmmuqXsn5TGoY/QwmnCU/YMnV74eKE2TSsn5TGoY/
E83j9WQhbUQXsn5T",
            "BlockIndex": 4
```

```
        },
        .....
        {
            "BlockToken": "yThPUAbQhb5V8xpwmnCU/
YMnV74eKE2TSFY1sKP/4r05y47WETdTONyThPUA",
            "BlockIndex": 12890
        },
        {
            "BlockToken":
 "ABgBASHKD5V8xEbaRKdxdkZZS4eKE2TSFYlMG1sKP/4r05y47WEHqKaNPcLs",
            "BlockIndex": 12906
        },
        {
            "BlockToken": "ABgBARROGMUJo6P9X3CFHQGZNQ7av9B6vZtTTqV89QqC
+SkO0HWMlwkGXjnA",
            "BlockIndex": 16383
        }
    ],
    "VolumeSize": 8,
    "ExpiryTime": 1637677800.845,
    "BlockSize": 524288
}
```

2. Encontre o volume de origem do qual o snapshot que você deseja arquivar foi criado. Use o comando describe-snapshots. Em `--snapshot-id`, especifique o ID do snapshot que você deseja arquivar. O parâmetro de resposta `VolumeId` indica o ID do volume de origem.

```
$ aws ec2 describe-snapshots --snapshot-id snapshot_id
```

Por exemplo, o comando a seguir retorna informações sobre o snapshot `snap-09c9114207084f0d9`.

```
$ aws ec2 describe-snapshots --snapshot-id snap-09c9114207084f0d9
```

A seguir está a saída do comando, que indica que esse snapshot `snap-09c9114207084f0d9` foi criado a partir do volume `vol-0f3e2c292c52b85c3`.

```
{
    "Snapshots": [
        {
            "Description": "",
```

```
            "Tags": [],
            "Encrypted": false,
            VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        }
    ]
}
```

3. Encontre todos os snapshots criados a partir do volume de origem. Use o comando describe-snapshots. Especifique o filtro `volume-id` e, para o valor do filtro, especifique o ID do volume da etapa anterior.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id, Values=volume_id"
```

Por exemplo, o comando a seguir retorna todos os snapshots criados a partir do volume `vol-0f3e2c292c52b85c3`.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id,
 Values=vol-0f3e2c292c52b85c3"
```

A seguir está a saída do comando, que indica que três snapshots foram criados a partir do volume `vol-0f3e2c292c52b85c3`.

```
{
    "Snapshots": [
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-14T08:57:39.300Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-08ca60083f86816b0"
```

```
        },
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-15T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        },
        {
            "Description": "01",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T07:50:08.042Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-024f49fe8dd853fa8"
        }
    ]
}
```

4. Usando a saída do comando anterior, classifique os snapshots por hora de criação, do mais antigo ao mais novo. O parâmetro de resposta `StartTime` para cada snapshot indica a hora de sua criação, no formato de hora UTC.

   Por exemplo, os snapshots retornados na etapa anterior, organizados por hora de criação, do mais antigo ao mais novo, são os seguintes:

   1. `snap-08ca60083f86816b0` (o mais antigo, criado antes do snapshot que você deseja arquivar)
   2. `snap-09c9114207084f0d9` (o snapshot a ser arquivado)
   3. `snap-024f49fe8dd853fa8` (o mais novo, criado depois do snapshot que você deseja arquivar)

5. Identifique os snapshots que foram criados imediatamente antes e depois do snapshot que você deseja arquivar. Nesse caso, você deseja arquivar o snapshot `snap-09c9114207084f0d9`, que foi o segundo snapshot incremental criado no conjunto de três snapshots. O snapshot `snap-08ca60083f86816b0` foi criado imediatamente antes e o snapshot `snap-024f49fe8dd853fa8` foi criado imediatamente depois.

6. Encontre os dados não referenciados no snapshot que você deseja arquivar. Primeiro, encontre os blocos que são diferentes entre o snapshot que foi criado imediatamente antes do snapshot que você deseja arquivar e o snapshot que você deseja arquivar. Use o comando list-changed-blocks. Em `--first-snapshot-id`, especifique o ID do snapshot criado imediatamente antes do snapshot que você deseja arquivar. Em `--second-snapshot-id`, especifique o ID do snapshot que você deseja arquivar.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_created_before --second-
snapshot-id snapshot_to_archive
```

Por exemplo, o comando a seguir mostra os índices de bloco para os blocos que são diferentes entre o snapshot `snap-08ca60083f86816b0` (o snapshot criado antes do snapshot que você deseja arquivar) e snapshot `snap-09c9114207084f0d9` (o snapshot que você deseja arquivar).

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-08ca60083f86816b0 --second-
snapshot-id snap-09c9114207084f0d9
```

A seguir está a saída do comando, com alguns blocos omitidos.

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAX6y
+WH6Rm9y5zq1VyeTCmEzGmTT0jNZG1cDirFq1rOVeFbWXsH3W4z/",
            "SecondBlockToken": "ABgBASyx0bHHBnTERu
+9USLxYK/81UT0dbHIUFqUjQUkwTwK5qkjP8NSGyNB",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAcfL
+EfmQmlNgstqrFnYgsAxR4SDSO4LkNLYOOChGBWcfJnpn90E9XX1",
```

```
            "SecondBlockToken": "ABgBAdX0mtX6aBAt3EBy
+8jFCESMpig7csKjbO2Ocd08m2iNJV2Ue+cRwUqF",
            "BlockIndex": 5
        },
        {
            "FirstBlockToken": "ABgBAVBaFJmbP/eRHGh7vnJlAwyiyNUi3MKZmEMxs2wC3AmM/
fc6yCOAMb65",
            "SecondBlockToken":
 "ABgBAdewWkHKTcrhZmsfM7GbaHyXD1Ctcn2nppz4wYItZRmAo1M72fpXU0Yv",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken": "ABgBAQGxwuf6z095L6DpRoVRVnOqPxmx9r7Wf6O+i
+ltZ0dwPpGN39ijztLn",
            "SecondBlockToken": "ABgBAUdlitCVI7c6hGsT4ckkKCw6bMRclnV
+bKjViu/9UESTcW7CD9w4J2td",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken":
 "ABgBAZBfEv4EHS1aSXTXxSE3mBZG6CNeIkwxpljzmgSHICGlFmZCyJXzE4r3",
            "SecondBlockToken":
 "ABgBAVWR7QuQQB0AP2TtmNkgS4Aec5KAQVCldnpc91zBiNmSfW9ouIlbeXWy",
            "BlockIndex": 15
        },
        .....
        {
            "SecondBlockToken": "ABgBAeHwXPL+z3DBLjDhwjdAM9+CPGV5VO5Q3rEEA
+ku50P498hjnTAgMhLG",
            "BlockIndex": 13171
        },
        {
            "SecondBlockToken":
 "ABgBAbZcPiVtLx6U3Fb4lAjRdrkJMwW5M2tiCgIp6ZZpcZ8AwXxkjVUUHADq",
            "BlockIndex": 13172
        },
        {
            "SecondBlockToken": "ABgBAVmEd/pQ9VW9hWiOujOAKcauOnUFCO
+eZ5ASVdWLXWWC04ijfoDTpTVZ",
            "BlockIndex": 13173
        },
        {
            "SecondBlockToken": "ABgBAT/jeN7w
+8ALuNdaiwXmsSfM6tOvMoLBLJ14LKvavw4IiB1d0iykWe6b",
```

```
            "BlockIndex": 13174
        },
        {
            "SecondBlockToken": "ABgBAXtGvUhTjjUqkwKXfXzyR2GpQei/
+pJSG/19ESwvt7Hd8GHaUqVs6Zf3",
            "BlockIndex": 13175
        }
    ],
    "ExpiryTime": 1637648751.813,
    "VolumeSize": 8
}
```

Em seguida, use o mesmo comando para encontrar os blocos que são diferentes entre o snapshot que você deseja arquivar e o snapshot que foi criado imediatamente depois dele. Em `--first-snapshot-id`, especifique o ID do snapshot que você deseja arquivar. Em `--second-snapshot-id`, especifique o ID do snapshot criado imediatamente depois do snapshot que você deseja arquivar.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_to_archive --second-
snapshot-id snapshot_created_after
```

Por exemplo, o comando a seguir mostra os índices de bloco dos blocos que são diferentes entre o snapshot `snap-09c9114207084f0d9` (o snapshot que você deseja arquivar) e o snapshot `snap-024f49fe8dd853fa8` (o snapshot criado depois do snapshot que você deseja arquivar).

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-09c9114207084f0d9 --second-
snapshot-id snap-024f49fe8dd853fa8
```

A seguir está a saída do comando, com alguns blocos omitidos.

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAVax0bHHBnTERu
+9USLxYK/81UT0dbSnkDk0gqwRFSFGWA7HYbkkAy5Y",
            "SecondBlockToken":
 "ABgBASEvi9x8Om7Htp37cKG2NT9XUzEbLHpGcayelomSoHpGy8LGyvG0yYfK",
```

```
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAeL0mtX6aBAt3EBy+8jFCESMpig7csfMrI4ufnQJT3XBm/
pwJZ1n2Uec",
            "SecondBlockToken": "ABgBAXmUTg6rAI
+v0LvekshbxCVpJjWILvxgC0AG0GQBEUNRVHkNABBwXLkO",
            "BlockIndex": 5
        },
        {
            "FirstBlockToken":
 "ABgBATKwWkHKTcrhZmsfM7GbaHyXD1CtcnjIZv9YzisYsQTMHfTfh4AhS0s2",
            "SecondBlockToken": "ABgBAcmiPFovWgXQio
+VBrxOqGy4PKZ9SAAHaZ2HQBM9fQQU0+EXxQjVGv37",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken":
 "ABgBAbRlitCVI7c6hGsT4ckkKCw6bMRclnARrMt1hUbIhFnfz8kmUaZOP2ZE",
            "SecondBlockToken": "ABgBAXe935n544+rxhJ0INB8q7pAeoPZkkD27vkspE/
qKyvOwpozYII6UNCT",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken": "ABgBAd+yxCO26I
+1Nm2KmuKfrhjCkuaP6LXuol3opCNk6+XRGcct4suBHje1",
            "SecondBlockToken": "ABgBAcPpnXz821NtTvWBPTz8uUFXnS8jXubvghEjZulIjHgc
+7saWys77shb",
            "BlockIndex": 18
        },
        .....
        {
            "SecondBlockToken": "ABgBATni4sDE5rS8/a9pqV03lU/lKCW
+CTxFl3cQ5p2f2h1njpuUiGbqKGUa",
            "BlockIndex": 13190
        },
        {
            "SecondBlockToken": "ABgBARbXo7zFhu7IEQ/9VMYFCTCtCuQ
+iSlWVpBIshmeyeS5FD/M0i64U+a9",
            "BlockIndex": 13191
        },
        {
            "SecondBlockToken": "ABgBAZ8DhMk+rROXa4dZlNK45rMYnVIGGSyTeiMli/sp/
JXUVZKJ9sMKIsGF",
```

```
            "BlockIndex": 13192
        },
        {
            "SecondBlockToken":
 "ABgBATh6MBVE904l6sqOC27s1nVntFUpDwiMcRWGyJHy8sIgGL5yuYXHAVty",
            "BlockIndex": 13193
        },
        {
            "SecondBlockToken":
 "ABgBARuZykaFBWpCWrJPXaPCneQMbyVgnITJqj4c1kJWPIj5Gn61OQyy+giN",
            "BlockIndex": 13194
        }
    ],
    "ExpiryTime": 1637692677.286,
    "VolumeSize": 8
}
```

7. Compare a saída retornada pelos dois comandos na etapa anterior. Se o mesmo índice de bloco aparecer nas saídas de ambos os comandos, isso indica que o bloco contém dados não referenciados.

   Por exemplo, a saídas do comando na etapa anterior indica que os blocos 4, 5, 13 e 14 são exclusivos do snapshot `snap-09c9114207084f0d9` e que eles não são referenciados por nenhum outro snapshot na linhagem do snapshot.

   Para determinar a redução em armazenamento na camada padrão, multiplique o número de blocos que aparecem nas saídas de ambos os comando por 512 KiB, que é o tamanho de bloco do snapshot.

   Por exemplo, se 9.950 índices de bloco aparecerem nas saídas de ambos os comandos, isso indica que você diminuirá o armazenamento no nível padrão em cerca de 4,85 GiB (9.950 blocos * 512 KiB = 4,85 GiB).

8. Determine os custos de armazenamento para armazenar os blocos não referenciados no nível padrão por 90 dias. Compare esse valor com o custo de armazenar o snapshot completo, descrito na etapa 1, no nível de arquivamento. É possível determinar sua economia de custos comparando os valores, supondo que não restaure o snapshot completo do nível de arquivo durante o período mínimo de 90 dias. Para obter mais informações, consulte Definição de preço e faturamento.

Permissões obrigatórias do IAM

Por padrão, os usuários não têm permissão para usar o arquivamento de snapshots. Para permitir que os usuários usem arquivamento de snapshots, crie políticas do IAM que concedam permissão para o uso dos recursos e ações de API específicos. Para obter mais informações, consulte Criar políticas do IAM no Guia do usuário do IAM.

Para usar o arquivamento de snapshots, os usuários precisam das permissões a seguir.

- `ec2:DescribeSnapshotTierStatus`
- `ec2:ModifySnapshotTier`
- `ec2:RestoreSnapshotTier`

Os usuários do console podem precisar de permissões adicionais, como `ec2:DescribeSnapshots`.

Para arquivar e restaurar instantâneos criptografados, são necessárias as seguintes permissões adicionais do AWS KMS.

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`

A seguir está um exemplo de política do IAM que dá aos usuários do IAM permissão para arquivar, restaurar e visualizar snapshots criptografados e não criptografados. Isso inclui a permissão `ec2:DescribeSnapshots` para usuários do console. Se algumas permissões não forem necessárias, você poderá removê-las da política.

> **Tip**
>
> Para seguir o princípio de menor privilégio, não permita acesso total a `kms:CreateGrant`. Em vez disso, use a chave de condição `kms:GrantIsForAWSResource` para permitir que o usuário crie concessões na chave do KMS somente quando a concessão for criada em nome do usuário por um serviço da AWS, conforme mostrado no exemplo a seguir.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeSnapshotTierStatus",
            "ec2:ModifySnapshotTier",
            "ec2:RestoreSnapshotTier",
            "ec2:DescribeSnapshots",
            "kms:CreateGrant",
            "kms:Decrypt",
            "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
    }]
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Trabalhar com arquivamento de snapshots

Tópicos

Arquivar um snapshot

É possível arquivar qualquer snapshot que você possua na sua conta que esteja no estado `completed`. Não é possível arquivar snapshots no estado `pending` ou `error`, nem os snapshots que são compartilhados com você. Para obter mais informações, consulte Considerações e limitações.

Se o snapshot estiver associado a uma ou mais AMIs, você deverá primeiro desabilitar essas AMIs associadas para que seja possível arquivá-lo. Para obter mais informações, consulte Desabilitar uma AMI.

Os snapshots arquivados retêm seu ID de snapshot, status de criptografia, permissões do AWS Identity and Access Management (IAM), informações do proprietário e tags de recursos. No entanto, a restauração rápida de snapshots e o compartilhamento de snapshots são desabilitados automaticamente depois que o snapshot é arquivado.

É possível continuar usando o snapshot enquanto ele está sendo arquivado. Assim que o status de classificação do snapshot em camadas atinge o estado de `archival-complete`, você não pode mais usar o snapshot.

É possível arquivar um snapshot usando um dos métodos a seguir.

Console

Para arquivar um snapshot

Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

1. No painel de navegação, selecione Snapshots.

2. Na lista de snapshots, selecione o snapshot a ser arquivado e escolha Actions (Ações), Archive snapshot (Arquivar snapshot).
3. Para confirmar, escolha Archive snapshot (Arquivar snapshot).

AWS CLI

Para arquivar um snapshot

Use o comando modify-snapshot-tier da AWS CLI. Em `--snapshot-id`, especifique o ID do snapshot a ser arquivado. Para `--storage-tier`, especifique `archive`.

```
$ aws ec2 modify-snapshot-tier \
--snapshot-id snapshot_id \
--storage-tier archive
```

Por exemplo, o comando a seguir arquiva o snapshot `snap-01234567890abcedf`.

```
$ aws ec2 modify-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--storage-tier archive
```

A seguir está saída do comando. O parâmetro de resposta `TieringStartTime` indica a data e hora em que o processo de arquivamento foi iniciado, no formato de hora UTC (AAAA-MM-DDTHH:MM:SSZ).

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "TieringStartTime": "2021-09-15T16:44:37.574Z"
}
```

Restaurar um snapshot arquivado

Antes de poder usar um snapshot arquivado, é necessário restaurá-lo para a camada padrão. O snapshot restaurado tem o mesmo ID de snapshot, status de criptografia, permissões do IAM, informações do proprietário e tags de recursos que tinha antes de ser arquivado. Depois de restaurado, é possível usá-lo como usa qualquer outro snapshot em sua conta. O snapshot restaurado é sempre um snapshot completo.

Quando você restaura um snapshot, pode escolher restaurá-lo permanentemente ou temporariamente.

Se você restaurar um snapshot permanentemente, ele será movido permanentemente da camada de arquivo para a camada padrão. O snapshot permanece restaurado e pronto para uso até você rearquivá-lo manualmente ou excluí-lo manualmente. Quando você restaura permanentemente um snapshot, ele é removido do nível de arquivo.

Se você restaurar um snapshot temporariamente, ele será copiado do nível de arquivo para o nível padrão por um período de restauração que você especifica. O snapshot permanece restaurado e pronto para uso somente durante o período de restauração. Durante o período de restauração, uma cópia do snapshot permanece no nível de arquivo. Após o período expirar, o snapshot é removido automaticamente do nível padrão. É possível aumentar ou diminuir o período de restauração, ou alterar o tipo de restauração para permanente a qualquer momento durante o período de restauração. Para obter mais informações, consulte Modificar o período de restauração ou o tipo de restauração para um snapshot restaurado temporariamente.

Se você estiver restaurando snapshots associados a uma AMI desabilitada e pretende usar essa AMI, primeiro restaure permanentemente todos os snapshots associados e, em seguida, reabilite uma AMI desabilitada para poder usá-la. Você não poderá habilitar uma AMI se os snapshots associados forem restaurados temporariamente. Você pode usar o comando a seguir para encontrar todos os snapshots associados a uma AMI.

```
$ C:\> aws ec2 describe-images --image-id ami_id \
  --query Images[*].BlockDeviceMappings[*].Ebs[].SnapshotId[]
```

É possível restaurar um snapshot arquivado usando um dos métodos a seguir.

Console

Para restaurar um snapshot do arquivo

Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

1. No painel de navegação, selecione Snapshots.
2. Na lista de snapshots, selecione o snapshot arquivado a ser restaurado e escolha Actions (Ações), Restore snapshot from archive (Restaurar o snapshot do arquivo).
3. Especifique o tipo de restauração a ser realizada. Em Restore type (Tipo de restauração), siga um destes procedimentos:

- Para restaurar o snapshot permanentemente, selecione Permanent (Permanente).
- Para restaurar o snapshot temporariamente, selecione Temporary (Temporária) e depois, para Temporary restore period (Período de restauração temporária), insira o número de dias pelos quais restaurar o snapshot.

4. Para confirmar, escolha Restore snapshot (Restaurar snapshot).

AWS CLI

Para restaurar permanentemente um snapshot arquivado

Use o comando restore-snapshot-tier da AWS CLI. Em `--snapshot-id`, especifique o ID do snapshot a ser restaurado e inclua a opção `--permanent-restore`.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snapshot_id \
--permanent-restore
```

Por exemplo, o comando a seguir restaura permanentemente o snapshot `snap-01234567890abcedf`.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--permanent-restore
```

A seguir está saída do comando.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

Para restaurar temporariamente um snapshot arquivado

Use o comando restore-snapshot-tier da AWS CLI. Omita a opção `--permanent-restore`. Em `--snapshot-id`, especifique o ID do snapshot a ser restaurado e, para `--temporary-restore-days`, especifique o número de dias pelos quais deseja restaurar o snapshot.

`--temporary-restore-days` deve ser especificado em dias. O intervalo permitido é de 1 a 180. Se você não especificar um valor, o padrão de 1 dia será adotado.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snapshot_id \
--temporary-restore-days number_of_days
```

Por exemplo, o comando a seguir restaura temporariamente o snapshot `snap-01234567890abcedf` por um período de restauração de 5 dias.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--temporary-restore-days 5
```

A seguir está saída do comando.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 5,
    "IsPermanentRestore": false
}
```

Modificar o período de restauração ou o tipo de restauração para um snapshot restaurado temporariamente

Quando você restaurar um snapshot temporariamente, deverá especificar o número de dias pelos quais o snapshot permanecerá restaurado em sua conta. Depois que o período de restauração expirar, o snapshot será removido automaticamente do nível padrão.

É possível alterar o período de restauração para um snapshot restaurado temporariamente a qualquer momento.

É possível escolher aumentar ou diminuir o período de restauração, ou pode alterar o tipo de restauração de temporário para permanente.

Se você alterar o período de restauração, o novo período de restauração estará em vigor a partir da data atual. Por exemplo, se você especificar um novo período de restauração de 5 dias, o snapshot permanecerá restaurado por cinco dias a partir da data atual.

> **Note**
> É possível encerrar uma restauração temporária com antecedência definindo o período de restauração como 1 dia.

Se você alterar o tipo de restauração de temporário para permanente, a cópia do snapshot será excluída do nível de arquivo e o snapshot permanecerá disponível em sua conta até ser rearquivado ou excluído manualmente.

É possível modificar o período de restauração de um snapshot usando um dos métodos a seguir.

Console

Para modificar o período de restauração ou o tipo de restauração

Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

1. No painel de navegação, selecione Snapshots.
2. Na lista de snapshots, selecione o snapshot que você restaurou temporariamente e escolha Actions (Ações), Restore snapshot from archive (Restaurar snapshot do arquivo).
3. Em Restore type (Tipo de restauração), siga um destes procedimentos:
   - Para alterar o tipo de restauração de temporário para permanente, selecione Permanent (Permanente).
   - Para aumentar ou diminuir o período de restauração, mantenha Temporary (Temporária) e, para Temporary restore period (Período de restauração temporária), insira o novo período de restauração em dias.
4. Para confirmar, escolha Restore snapshot (Restaurar snapshot).

AWS CLI

Para modificar o período de restauração ou alterar o tipo de restauração

Use o comando restore-snapshot-tier da AWS CLI. Em `--snapshot-id`, especifique o ID do snapshot que você restaurou temporariamente. Para alterar o tipo de restauração de temporária para permanente, especifique `--permanent-restore` e omita `--temporary-restore-days`. Para aumentar ou diminuir o período de restauração, omita `--permanent-restore` e, em `--temporary-restore-days`, especifique o novo período de restauração em dias.

Exemplo: aumentar ou diminuir o período de restauração

O comando a seguir altera o período de restauração do snapshot `snap-01234567890abcedf` para `10` dias.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf
--temporary-restore-days 10
```

A seguir está saída do comando.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 10,
    "IsPermanentRestore": false
}
```

Exemplo: alterar o tipo de restauração para permanente

O comando a seguir altera o tipo de restauração do snapshot `snap-01234567890abcedf` de temporária para permanente.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf
--permanent-restore
```

A seguir está saída do comando.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

Exibir snapshots arquivados

É possível visualizar informações da camada de armazenamento para snapshots usando um dos métodos a seguir.

Console

Para visualizar informações do nível de armazenamento para um snapshot

Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

1. No painel de navegação, selecione Snapshots.
2. Na lista de snapshots, selecione o snapshot e escolha a guia Storage tier (Nível de armazenamento).

   A tabela fornece as seguintes informações:

   - Início da última alteração do nível: a data e a hora de início do último arquivamento ou restauração.
   - Andamento da alteração do nível: o andamento da última ação de arquivamento ou restauração, como um percentual.
   - Nível de armazenamento: o nível de armazenamento para o snapshot. Sempre `archive` para snapshots arquivados e `standard` para snapshots armazenados no nível padrão, incluindo os snapshots restaurados temporariamente.
   - Status do nível: o status da última ação de arquivamento ou restauração.
   - Arquivamento concluído em: a data e a hora em que o arquivamento foi concluído.
   - A data de expiração da restauração temporária: a data e a hora em que um snapshot restaurado temporariamente está definido para expirar.

AWS CLI

Para visualizar informações de arquivamento sobre um snapshot arquivado

Use o comando describe-snapshot-tier-status da AWS CLI. Especifique o filtro `snapshot-id` e, para o valor do filtro, especifique o ID do snapshot. Ou então, para visualizar todos os snapshots arquivados, omita o filtro.

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
 Values=snapshot_id"
```

A saída inclui os seguintes parâmetros de resposta:

- `Status`: o status do snapshot. Sempre `completed` para os snapshots arquivados. Somente os snapshots que estão no estado `completed` podem ser arquivados.
- `LastTieringStartTime`: a data e hora em que o processo de arquivamento começou, no formato de hora UTC (AAAA-MM-DDTHH:MM:SSZ).
- `LastTieringOperationState`: o estado atual do processo de arquivamento. Os possíveis estados incluem: `archival-in-progress` | `archival-completed` | `archival-failed` | `permanent-restore-in-progress` | `permanent-restore-completed` | `permanent-restore-failed` | `temporary-restore-in-progress` | `temporary-restore-completed` | `temporary-restore-failed`
- `LastTieringProgress`: o andamento do processo de arquivamento dos snapshots, como um percentual.
- `StorageTier`: a camada de armazenamento para o snapshot. Sempre `archive` para snapshots arquivados e `standard` para snapshots armazenados no nível padrão, incluindo os snapshots restaurados temporariamente.
- `ArchivalCompleteTime`: a data e a hora em que o processo de arquivamento foi concluído, no formato de hora UTC (AAAA-MM-DDTHH:MM:SSZ).

Exemplo

O comando a seguir sempre exibe informações sobre o snapshot `snap-01234567890abcedf`.

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
 Values=snap-01234567890abcedf"
```

A seguir está saída do comando.

```
{
    "SnapshotTierStatuses": [
        {
            "Status": "completed",
            "ArchivalCompleteTime": "2021-09-15T17:33:16.147Z",
            "LastTieringProgress": 100,
            "Tags": [],
            "VolumeId": "vol-01234567890abcedf",
            "LastTieringOperationState": "archival-completed",
            "StorageTier": "archive",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890abcedf",
```

```
            "LastTieringStartTime": "2021-09-15T16:44:37.574Z"
        }
    ]
}
```

Para visualizar os snapshots arquivados e os snapshots no nível padrão

Use o comando describe-snapshot da AWS CLI. Em `--snapshot-ids`, especifique o ID do snapshot a ser exibido.

```
$ aws ec2 describe-snapshots --snapshot-ids snapshot_id
```

Por exemplo, o comando a seguir exibe informações sobre o snapshot `snap-01234567890abcedf`.

```
$ aws ec2 describe-snapshots --snapshot-ids snap-01234567890abcedf
```

A seguir está saída do comando. O parâmetro de resposta `StorageTier` indica se o snapshot está arquivado no momento, `archive` indica que o snapshot está arquivado no momento e armazenado no nível de arquivo, e `standard` indica que o snapshot não está arquivado no momento e que está armazenado no nível padrão.

No seguinte exemplo de saída, somente `Snap A` está arquivado, `Snap B` e `Snap C` não estão arquivados.

Além disso, o parâmetro de resposta `RestoreExpiryTime` é retornado somente para os snapshots que são restaurados temporariamente do arquivo. Ele indica quando os snapshots restaurados temporariamente devem ser removidos automaticamente do nível padrão. Ele não é retornado para snapshots que foram restaurados permanentemente.

No seguinte exemplo de saída, `Snap C` é restaurado temporariamente e será automaticamente removido do nível padrão em 2021-09-19T 21:00:00.000Z (19 de setembro de 2021 às 21:00 UTC).

```
{
    "Snapshots": [
        {
            "Description": "Snap A",
            "Encrypted": false,
            "VolumeId": "vol-01234567890aaaaaa",
```

```
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-09-07T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890aaaaaa",
            "StorageTier": "archive",
            "Tags": []
        },
        {
            "Description": "Snap B",
            "Encrypted": false,
            "VolumeId": "vol-09876543210bbbbbb",
            "State": "completed",
            "VolumeSize": 10,
            "StartTime": "2021-09-14T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09876543210bbbbbb",
            "StorageTier": "standard",
            "RestoreExpiryTime": "2019-09-19T21:00:00.000Z",
            "Tags": []
        },
        {
            "Description": "Snap C",
            "Encrypted": false,
            "VolumeId": "vol-054321543210cccccc",
            "State": "completed",
            "VolumeSize": 12,
            "StartTime": "2021-08-01T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-054321543210cccccc",
            "StorageTier": "standard",
            "Tags": []
        }
    ]
}
```

Para visualizar apenas os snapshots armazenados no nível de arquivamento ou no nível padrão

Use o comando describe-snapshot da AWS CLI. Inclua a opção `--filter`, para o nome do filtro, especifique `storage-tier` e, para o valor do filtro, especifique `archive` ou `standard`.

```
$ aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive|standard"
```

Por exemplo, o comando a seguir exibe apenas os snapshots arquivados.

```
$ aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive"
```

Monitorar o arquivamento de snapshots

O Amazon EBS emite eventos relacionados a ações de arquivamento de snapshots. É possível usar o AWS Lambda e o Amazon CloudWatch Events para tratar as notificações de eventos de forma programática. Eventos são emitidos com base no melhor esforço. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Events.

Os seguintes eventos estão disponíveis:

- `archiveSnapshot`: emitido quando uma ação de arquivamento de snapshot tem êxito ou falha.

  A seguir está um exemplo de um evento emitido quando uma ação de arquivamento de snapshots tem êxito.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Snapshot Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "2021-05-25T13:12:22Z",
   "region": "us-east-1",
   "resources": [
     "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
   ],
   "detail": {
     "event": "archiveSnapshot",
     "result": "succeeded",
     "cause": "",
     "request-id": "123456789",
     "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
     "startTime": "2021-05-25T13:12:22Z",
     "endTime": "2021-05-45T15:30:00Z",
     "recycleBinExitTime": "2021-10-45T15:30:00Z"
```

```
  }
```

A seguir está um exemplo de um evento emitido quando uma ação de arquivamento de snapshots falha.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "archiveSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `permanentRestoreSnapshot`: emitido quando uma ação de restauração permanente tem êxito ou falha.

  A seguir está um exemplo de um evento emitido quando uma ação de restauração permanente tem êxito.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
```

```
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-10-45T15:30:00Z"
  }
}
```

A seguir está um exemplo de um evento emitido quando uma ação de restauração permanente falha.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `temporaryRestoreSnapshot`: emitido quando uma ação de restauração temporária tem êxito ou falha.

A seguir está um exemplo de um evento emitido quando uma ação de restauração temporária tem êxito.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "restoreExpiryTime": "2021-06-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

A seguir está um exemplo de um evento emitido quando uma ação de restauração temporária falha.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
```

```
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `restoreExpiry`: emitido quando o período de restauração de um snapshot restaurado temporariamente expira.

  Veja um exemplo a seguir.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "restoryExpiry",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

Excluir um snapshot do Amazon EBS

Depois de não precisar mais de um snapshot do Amazon EBS de um volume, será possível excluí-lo. A exclusão de um snapshot não tem efeito sobre o volume. A exclusão de um volume não afeta os snapshots feitos com base nele.

Exclusão incremental de snapshot

Se você gera snapshots periódicos de um volume, eles são incrementais. Isso significa que somente os blocos do dispositivo que foram modificados depois do último snapshot são salvos no novo snapshot. Mesmo que os snapshots sejam salvos de forma incremental, o processo de exclusão de snapshots foi projetado de forma que você precise reter somente o snapshot mais recente a fim de criar volumes.

Se os dados estivessem presentes em um volume mantido em um snapshot anterior ou em uma série de instantâneos e esses dados forem posteriormente excluídos do volume posteriormente, os dados ainda serão considerados dados exclusivos dos snapshots anteriores. Os dados exclusivos serão excluídos da sequência de snapshots apenas se todos os snapshots que fazem referência aos dados exclusivos forem excluídos.

Ao excluir um snapshot, somente os dados mencionados exclusivamente por esse snapshot são removidos. Os dados exclusivos só serão excluídos se todos os snapshots que fazem referência a eles forem excluídos. A exclusão de snapshots anteriores de um volume não afeta sua capacidade de criar volumes de snapshots posteriores desse volume.

A exclusão de um snapshot pode não reduzir os custos de armazenamento de dados de sua organização. Outros snapshots podem fazer referência aos dados desse snapshot e os dados referenciados serão sempre preservados. Se você excluir um snapshot contendo dados usados por um snapshot mais recente, os custos associados aos dados referenciados são alocados ao snapshot posterior. Para obter mais informações sobre como os snapshots armazenam dados, consulte Como funcionam os snapshots e o exemplo a seguir.

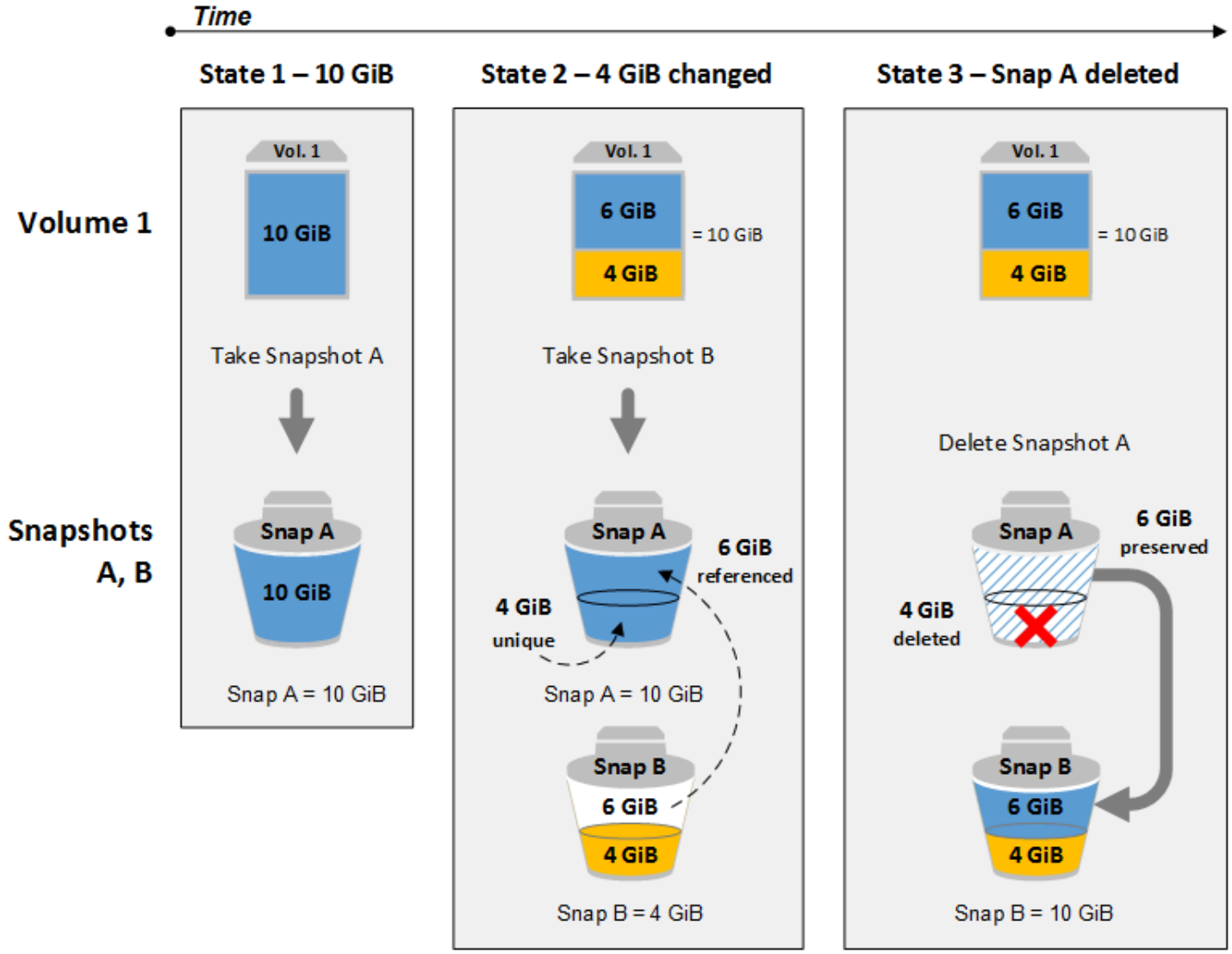
No diagrama a seguir, Volume 1 é mostrado em três pontos no tempo. Um snapshot capturou os dois primeiros estados e, no terceiro, um snapshot foi excluído.

- No estado 1, o volume tem 10 GiB de dados. Como Snap A é o primeiro snapshot criado do volume, todos os 10 GiB de dados devem ser copiados.
- No Estado 2, o volume ainda contém 10 GiB de dados, mas 4 GiB mudaram. O Snap B precisa copiar e armazenar somente os 4 GiB que mudaram após o Snap A ser tirado. Os outros 6 GiB de

dados inalterados, que já estão copiados e armazenados no Snap A, são consultados pelo Snap B vez de (novamente) copiados. Isso é indicado pela seta tracejada.

- No estado 3, o volume não foi alterado desde o Estado 2, mas o Snapshot A foi excluído. Os 6 GiB de dados armazenados no Snapshot A que foram mencionados pelo Snapshot B foram movidos para o Snapshot B, como mostrado pela seta preenchida. Como resultado, será cobrado de você ainda o armazenamento de 10 GiB de dados – 6 GiB de dados inalterados preservados do Snap A e 4 GiB de dados alterados do Snap B.

Exclusão de um snapshot com alguns de seus dados mencionados por outro snapshot



Considerações

As seguintes considerações se aplicam à exclusão de snapshots:

- Você não pode excluir um snapshot do dispositivo raiz de um volume do EBS usado por um AMI registrado. Essa consideração se aplica mesmo se a AMI registrada for descontinuada ou desabilitada. É necessário primeiro cancelar a AMI antes de excluir o snapshot. Para obter mais informações, consulte Cancelar o registro da sua AMI.
- Você não pode excluir um snapshot gerenciado pelo AWS Backup serviço usando o Amazon EC2. Em vez disso, use AWS Backup para excluir os pontos de recuperação correspondentes no cofre de backup. Para obter mais informações, consulte Exclusão de namespaces no Guia do desenvolvedor do AWS Backup .
- É possível criar, reter e excluir snapshots manualmente ou usar o Amazon Data Lifecycle Manager para gerenciar os snapshots para você. Para obter mais informações, consulte Amazon Data Lifecycle Manager.
- Embora você possa excluir um snapshot que ainda está em andamento, o snapshot deve ser concluído antes de a exclusão entrar em vigor. Isso pode levar muito tempo. Se você também estiver no limite de snapshots simultâneos e tentar criar um snapshot adicional, poderá obter o erro `ConcurrentSnapshotLimitExceeded`. Para obter mais informações, consulte Service Quotas para o Amazon EBS no Referência geral da Amazon Web Services.
- Se você excluir um instantâneo que corresponda a uma regra de retenção da Lixeira, o instantâneo será retido na Lixeira em vez de ser excluído imediatamente. Para obter mais informações, consulte Lixeira.
- Não é possível excluir os snapshots associados às AMIs desabilitadas baseadas em EBS. Para obter mais informações, consulte Desabilitar uma AMI.
- Você não pode excluir instantâneos compartilhados com você.
- Se você excluir um instantâneo compartilhado de sua propriedade, todas as contas com as quais o instantâneo é compartilhado perderão acesso a ele.

Excluir um snapshot

Para excluir um snapshot, use um dos métodos a seguir.

Console

Para excluir um snapshot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.

3. Selecione o snapshot a ser excluído e escolha Actions (Ações), Delete snapshot (Excluir snapshot).
4. Escolha Excluir.

AWS CLI

Para excluir um instantâneo usando o AWS CLI

Use o comando delete-snapshot.

Tools for Windows PowerShell

Para excluir um instantâneo usando as Ferramentas para Windows PowerShell

Use o comando Remove-EC2Snapshot.

> **Dica de solução de problemas**
>
> Se você receber um erro `Failed to delete snapshot` indicando que o snapshot está sendo usado atualmente por uma AMI, será necessário cancelar o registro da AMI associada antes de excluir o snapshot. Você não pode bloquear snapshots associados a uma AMI. Se você estiver usando o console e a AMI associada estiver desabilitada, deverá selecionar o filtro Imagens desabilitadas na tela AMIs para visualizar as AMIs desabilitadas.

Excluir um snapshot de vários volumes

Para excluir snapshots de vários volumes, recupere todos os snapshots do conjunto de snapshots de vários volumes usando a etiqueta aplicada ao conjunto quando os snapshots foram criados. Depois, exclua os snapshots individualmente.

A exclusão de snapshots individuais no conjunto de snapshots de vários volumes não será impedida. Se você excluir um snapshot enquanto ele estiver no `pending state`, somente esse snapshot será excluído. Os outros snapshots do conjunto de instantâneos de vários volumes ainda serão concluídos corretamente.

Automatizar o ciclo de vida do snapshot

É possível usar o Amazon Data Lifecycle Manager para automatizar a criação, retenção e exclusão de snapshots usados para fazer backup de seus volumes do Amazon EBS.

Para ter mais informações, consulte Amazon Data Lifecycle Manager.

Restauração rápida de snapshots do Amazon EBS

A restauração rápida de snapshots (FSR) do Amazon EBS permite criar um volume de um snapshot que está totalmente inicializado na criação. Isso elimina a latência das operações de E/S em um bloco quando ele é acessado pela primeira vez. Os volumes criados usando a restauração rápida de snapshots viabilizam instantaneamente toda a sua performance provisionada.

Para iniciar, habilite a restauração rápida de snapshots específicos em zonas de disponibilidade determinadas. Cada par de snapshots e zonas de disponibilidade refere-se a uma restauração rápida de snapshot. Ao criar um volume de um desses snapshots em uma de suas zonas de disponibilidade habilitadas, o volume é restaurado usando a restauração rápida de snapshot.

A restauração rápida do snapshot deve ser habilitada explicitamente por snapshot. Se você criar um novo snapshot de um volume que foi restaurado de um snapshot habilitado para restauração rápida, o novo snapshot não será ativado automaticamente para restauração rápida de snapshots. É necessário habilitá-lo explicitamente para o novo snapshot.

O número de volumes que é possível restaurar com todo o benefício da performance da restauração rápida de snapshots é determinado pelos créditos de criação de volume para o snapshot. Para obter mais informações, consulte Créditos de criação de volume.

É possível habilitar a restauração rápida de snapshots que você possui e de snapshots públicos e privados compartilhados com você.

Conteúdo

Considerações

- A restauração rápida de snapshots não é compatível com o AWS Outposts, zonas locais e zonas do Wavelength.
- A restauração rápida de snapshots pode ser habilitada em snapshots com um tamanho de 16 TiB ou menos.
- Os volumes provisionados com performance de até 64.000 IOPS e throughput de 1.000 MiB/s recebem o benefício total da performance de restauração rápida de snapshots. Para volumes provisionados com performance superior a 64.000 IOPS ou throughput de 1.000 MiB/s, recomendamos que você inicialize o volume para receber a performance total.

Créditos de criação de volume

O número de volumes que recebem todo o benefício da performance da restauração rápida de snapshots é determinado pelos créditos de criação de volume para o snapshot. Existe um bucket de crédito por snapshot por zona de disponibilidade. Cada volume criado a partir de um snapshot com restauração rápida de snapshots consome um crédito do bucket de crédito. É necessário ter pelo menos um crédito no bucket para criar um volume inicializado com base no snapshot. Se você criar um volume, mas houver menos de um crédito no bucket, o volume será criado sem o benefício da restauração rápida de snapshots.

Quando você habilita a restauração rápida de snapshots para um snapshot compartilhado com você, você obtém um bucket de crédito separado para o snapshot compartilhado em sua conta. Se você criar volumes do snapshot compartilhado, os créditos serão consumidos de seu bucket de crédito; eles não serão consumidos do bucket de crédito do proprietário do snapshot.

O tamanho do bucket de crédito e a taxa com a qual ele será reabastecido depende do tamanho do snapshot, não do tamanho dos volumes criados a partir do snapshot.

Quando você habilita a restauração rápida de snapshots para um snapshots, o bucket de crédito começa com zero créditos e é preenchido a uma taxa definida até atingir sua capacidade máxima de crédito. Além disso, à medida que você consome créditos, o bucket de crédito é reabastecido com o tempo até atingir sua capacidade máxima de crédito.

A velocidade de reabastecimento de cada bucket de crédito é calculada da seguinte forma:

```
MIN (10, (1024 ÷ snapshot_size_gib))
```

E o tamanho do bucket de crédito é calculado da seguinte forma:

```
MAX (1, MIN (10, (1024 ÷ snapshot_size_gib)))
```

Por exemplo, se você habilitar a restauração rápida de um snapshot com um tamanho de `128 GiB`, a taxa de abastecimento é de `0.1333` créditos por minuto.

```
MIN (10, (1024 ÷ 128))
 = MIN (10, 8)
 = 8 credits per hour
 = 0.1333 credits per minute
```

E o tamanho máximo do bucket de crédito é de 8 créditos.

```
MAX (1, MIN (10, (1024 ÷ 128)))
 = MAX (1, MIN (10, 8))
 = MAX (1, 8)
 = 8 credits
```

Neste exemplo, quando você habilita a restauração rápida de snapshots, o bucket de crédito começa com zero créditos. Após 8 minutos, o bucket de crédito tem créditos suficientes para criar um volume inicializado (`0.1333 credits × 8 minutes = 1.066 credits`). Quando o bucket de crédito estiver cheio, será possível criar 8 volumes inicializados simultaneamente (8 créditos). Quando o bucket está abaixo de sua capacidade máxima, ele reabastece com `0.1333` créditos por minuto.

É possível usar métricas do CloudWatch para monitorar o tamanho dos buckets de crédito e o número de créditos disponíveis em cada bucket. Para obter mais informações, consulte Métricas para a restauração rápida do snapshot.

Após criar um volume de um snapshot com a restauração rápida de snapshots habilitada, será possível descrever o volume usando describe-volumes e verificar o campo `fastRestored` na saída para determinar se o volume foi criado como um volume inicializado usando a restauração rápida de snapshots.

Gerenciar a restauração rápida de snapshots

Tópicos

- Habilitar ou desabilitar a restauração rápida de snapshot
- Exibir o estado de restauração de um snapshot

- Exibir volumes restaurados usando restauração rápida de snapshot

Habilitar ou desabilitar a restauração rápida de snapshot

Por padrão, a restauração rápida de snapshots está desabilitada para um snapshot. É possível habilitar ou desabilitar a restauração rápida de snapshots para snapshots que você possui e que são compartilhados com você. Quando você habilita ou desabilita a restauração rápida de snapshots para um snapshot, as alterações se aplicam somente à sua conta.

> **Note**
>
> Quando você habilita a restauração rápida de snapshots para um snapshot, sua conta é cobrada por cada minuto em que a restauração rápida de snapshots está habilitada em uma determinada zona de disponibilidade. As cobranças são proporcionais, com um mínimo de uma hora.

Quando você exclui um snapshot que você possui, a restauração rápida de snapshots é automaticamente desabilitada para esse snapshot em sua conta. Se você habilitou a restauração rápida de snapshots para um snapshot compartilhado com você, e o proprietário do snapshot excluí-lo ou descompartilhá-lo, a restauração rápida de snapshots será automaticamente desabilitada para o snapshot compartilhado em sua conta.

Se você habilitou a restauração rápida de snapshots para um snapshot compartilhado com você e ele for criptografado usando uma CMK personalizada, a restauração rápida de snapshots não será desabilitada automaticamente para o snapshot quando o proprietário do snapshot revogar seu acesso à CMK personalizada. É necessário desabilitar manualmente a restauração rápida de snapshots para esse snapshot.

Use os métodos a seguir para habilitar ou desabilitar a restauração rápida de snapshots para um snapshot que você possui ou para um snapshot compartilhado com você.

Console

Como habilitar ou desabilitar a restauração rápida de snapshot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.

3. Selecione o snapshot e escolha Actions (Ações), Manage fast snapshot restore (Gerenciar a restauração rápida de snapshot).
4. A seção Configurações de restauração rápida de snapshots lista todas as zonas de disponibilidade nas quais é possível habilitar a restauração rápida de snapshots para o snapshot selecionado. O volume Current status (Status atual) indica se a restauração rápida de snapshots está habilitada ou desabilitada para cada zona.

   Para habilitar a restauração rápida de snapshots em uma zona onde ela está atualmente desabilitada, selecione a zona, escolha Enable (Habilitar) e, para confirmar, escolha Enable (Habilitar).

   Para desabilitar a restauração rápida de snapshots em uma zona onde ela está habilitada atualmente, selecione a zona e, em seguida, escolha Disable (Desabilitar).
5. Depois de fazer as alterações necessárias, escolha Close (Fechar).

AWS CLI

Para gerenciar a restauração rápida de snapshots usando a AWS CLI

- enable-fast-snapshot-restores
- disable-fast-snapshot-restores
- describe-fast-snapshot-restores

> **Note**
>
> Depois que você habilitar a restauração rápida para um snapshot, ele entrará no estado `optimizing`. Os snapshots que estão no estado `optimizing` oferecem alguns benefícios de performance ao usá-los para restaurar volumes. Eles passam a oferecer os benefícios de performance total da restauração rápida de snapshots somente depois de entrarem no estado `enabled`.

Exibir o estado de restauração de um snapshot

A restauração rápida para um snapshot pode estar em um dos estados a seguir.

- `enabling` — foi feita uma solicitação para habilitar a restauração rápida de snapshots.

- `optimizing` — a restauração rápida de snapshots está sendo habilitada. Demora 60 minutos por TiB para otimizar um snapshot. Os snapshots nesse estado oferecem alguns benefícios de performance ao restaurar volumes.
- `enabled` — a restauração rápida de snapshots está habilitada. Os snapshots nesse estado e com créditos de criação de volume suficientes oferecem o benefício de desempenho total ao restaurar volumes.
- `disabling` — foi feita uma solicitação para desabilitar a restauração rápida de snapshots ou houve falha em uma solicitação para habilitar a restauração rápida de snapshots.
- `disabled` — a restauração rápida de snapshots está desabilitada. É possível reabilitar a restauração rápida de snapshots, se necessário.

Use um dos métodos a seguir para exibir o estado da restauração rápida de snapshots para um snapshot que você possui ou para um snapshot compartilhado com você.

Console

Como visualizar o estado da restauração rápida do snapshot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot.
4. Na guia Detais (Detalhes), Fast Snapshot Restore (Restauração rápida de snapshots) indica o estado da restauração rápida do snapshot.

AWS CLI

Como visualizar snapshots com restauração rápida habilitada com a AWS CLI

Use o comando describe-fast-snapshot-restores para descrever os snapshots habilitados para restauração rápida.

```
aws ec2 describe-fast-snapshot-restores --filters Name=state,Values=enabled
```

A seguir está um exemplo de saída.

```
{
    "FastSnapshotRestores": [
```

```
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2a",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        },
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2b",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        }
    ]
}
```

Exibir volumes restaurados usando restauração rápida de snapshot

Ao criar um volume de um snapshot habilitado para restauração rápida na zona de disponibilidade para o volume, ele é restaurado usando a restauração rápida de snapshot.

Use o comando describe-volumes para visualizar volumes criados a partir de um snapshot habilitado para restauração rápida.

```
aws ec2 describe-volumes --filters Name=fast-restored,Values=true
```

A seguir está um exemplo de saída.

```
{
    "Volumes": [
        {
            "Attachments": [],
            "AvailabilityZone": "us-east-2a",
```

```
            "CreateTime": "2020-01-26T00:34:11.093Z",
            "Encrypted": true,
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-
a87a-5513e232e843",
            "Size": 20,
            "SnapshotId": "snap-0e946653493cb0447",
            "State": "available",
            "VolumeId": "vol-0d371921d4ca797b0",
            "Iops": 100,
            "VolumeType": "gp2",
            "FastRestored": true
        }
    ]
}
```

Monitorar a restauração rápida de snapshot

O Amazon EBS emite eventos do Amazon CloudWatch quando o estado de restauração de um snapshot é alterado. Para obter mais informações, consulte Eventos de restauração rápida do snapshot do EBS.

Cotas de restauração rápida de snapshots

É possível habilitar até cinco snapshots para restauração rápida de snapshots por região. A cota se aplica aos snapshots que você possui e aos snapshots compartilhados com você. Se você habilitar a restauração rápida de um snapshot compartilhado com você, ela será contada em sua cota de restauração rápida de snapshots. Ela não será contada na cota de restauração rápida de snapshots do proprietário do snapshot.

Definição de preço e cobrança

Você será cobrado por cada minuto em que a restauração rápida de snapshots estiver habilitada para um snapshot em uma determinada zona de disponibilidade. As cobranças são divididas com um mínimo de uma hora.

Por exemplo, se você habilitar a restauração rápida de snapshots para um snapshot em `US-East-1a` por um mês (30 dias), será cobrado em USD 540 (1 snapshot x 1 AZ x `720` horas x `$0.75` por hora). Se você habilitar a restauração rápida de snapshots para dois snapshots em `us-east-1a`, `us-east-1b`, e `us-east-1c` para o mesmo período, você será cobrado em USD 3.240 (2 snapshots x 3 AZs x `720` horas x `$0.75` por hora).

Se você habilitar a restauração rápida de snapshots para um snapshot público ou privado compartilhado com você, sua conta será cobrada. O proprietário do snapshot não será cobrado. Quando um snapshot compartilhado com você é excluído ou não compartilhado pelo proprietário do snapshot, a restauração rápida do snapshots é desabilitada para o snapshot em sua conta, e o faturamento é interrompido.

Para obter mais informações, consulte Definição de preço do Amazon EBS.

Bloqueio de snapshots do Amazon EBS

Você pode bloquear seus snapshots do Amazon EBS para protegê-los contra exclusões acidentais ou maliciosas ou armazená-los no formato WORM (write-once-read-many) por um período específico. Enquanto um snapshot está bloqueado, ele não pode ser excluído por nenhum usuário, independentemente das permissões do IAM. Você pode continuar a usar um snapshot bloqueado como usaria qualquer outro snapshot.

> **Note**
>
> O bloqueio de snapshots foi avaliado pela Cohasset Associates para uso em ambientes sujeitos aos regulamentos SEC 17a-4, CFTC e FINRA. Para obter mais informações sobre como o bloqueio de snapshots está relacionado com essas regulamentações, consulte Cohasset Associates Compliance Assessment.

Você pode bloquear snapshots em um de dois modos: modo de conformidade ou modo de governança e eles podem ser bloqueados por um período específico ou até uma data específica. Para obter mais informações, consulte Modo de bloqueio e Duração do bloqueio.

Definição de preço

Você pode bloquear e desbloquear snapshots sem nenhum custo adicional. Você paga os custos padrão de armazenamento de snapshots do Amazon EBS pelos snapshots bloqueados.

Tópicos

- Monitore bloqueios de snapshots do Amazon EBS usando AWS CloudTrail
- Monitore bloqueios de snapshots do Amazon EBS usando a Amazon EventBridge

Bloqueio de snapshots do Amazon EBS

Veja a seguir conceitos importantes que você deve entender ao começar a usar o bloqueio de snapshots.

Sumário

Modo de bloqueio

Você pode bloquear um snapshot em um dos dois modos:

Modo de governança

Depois que um snapshot é bloqueado, os usuários com as permissões apropriadas do IAM podem desbloquear o snapshot e modificar o modo de bloqueio e a duração ou a data de expiração do bloqueio a qualquer momento. Quando você bloqueia um snapshot no modo de governança, o snapshot é bloqueado imediatamente; não existe um período de desistência. Para excluir um snapshot após ele ter sido bloqueado no modo de governança, você deve primeiro desbloquear o snapshot ou deve esperar que o bloqueio expire.

Você pode usar o modo de governança para atender aos requisitos de governança de dados da sua organização, garantindo que somente determinados usuários tenham permissão para desbloquear snapshots e modificar as configurações de bloqueio de snapshots. Também é possível usar o modo de governança para testar a configuração do bloqueio antes de bloquear um snapshot no modo de conformidade.

Modo de conformidade

Ao bloquear um snapshot no modo de conformidade, você pode, opcionalmente, especificar um período de desistência que começa imediatamente após o bloqueio do snapshot. Durante o período

de desistência, os usuários com as permissões apropriadas podem desbloquear o snapshot, alterar o modo de bloqueio, aumentar ou diminuir o período de desistência e aumentar ou diminuir a duração do bloqueio ou sua data de expiração. Depois que o período de desistência expira, você não pode desbloquear o snapshot, alterar o modo de bloqueio nem diminuir a duração ou a data de expiração do bloqueio; você só pode aumentar a duração ou adiar a data de expiração do bloqueio. Para excluir um snapshot depois que ele bloqueado no modo de conformidade e que período de desistência terminou, você deve esperar que o bloqueio expire.

> **Note**
>
> Você pode bloquear um snapshot no modo de conformidade sem um período de desistência, omitindo o período de desistência na solicitação. Se você fizer isso, o bloqueio passará a vigorar imediatamente e não será mais possível desbloquear o snapshot, alterar o modo de bloqueio nem diminuir a duração ou antecipar a data de expiração do bloqueio; você só pode aumentar a duração ou a adiar a data de expiração do bloqueio.

Você pode usar o modo de conformidade para proteger os snapshots que não devem ser excluídos por um período específico por motivos de conformidade. O modo de conformidade oferece os seguintes benefícios:

- Ele habilita a configuração WORM (write once, read-many) para seus snapshots.
- Ele fornece uma camada adicional de defesa que protege os snapshots contra exclusões acidentais ou maliciosas.
- Ele impõe períodos de retenção, que evitam exclusões antecipadas por usuários privilegiados, para atender às políticas e procedimentos de proteção de dados da sua organização.

> **Note**
>
> A única maneira de excluir um snapshot bloqueado no modo de conformidade antes que o bloqueio expire é fechar a conta associada AWS .

Duração do bloqueio

A duração do bloqueio é o período durante o qual o snapshot deve permanecer bloqueado. É possível especificar a duração do bloqueio como uma das opções a seguir, mas não ambas:

Número de dias

A duração do bloqueio é especificada como o número de dias durante os quais o snapshot permanecerá bloqueado. Depois de decorrido o número especificado de dias, o snapshot é automaticamente desbloqueado. A duração pode variar de 1 dia a 36.500 dias (100 anos).

Data de expiração do bloqueio

A duração do bloqueio é determinada por uma data de expiração no futuro. O snapshot permanece bloqueado até que a data de expiração do bloqueio seja atingida. Quando a data de expiração do bloqueio é atingida, o snapshot é desbloqueado automaticamente.

Período de desistência

O período de desistência é um período opcional que você pode especificar ao bloquear um snapshot no modo de conformidade. Durante o período de desistência, os usuários com as permissões apropriadas podem desbloquear o snapshot, alterar o modo de bloqueio, aumentar ou diminuir o período de desistência, aumentar ou diminuir a duração do bloqueio e antecipar ou adiar a sua data de expiração. Depois que o período de desistência expira, os usuários não podem mais desbloquear o snapshot, alterar o modo de bloqueio, restabelecer o período de desistência ou diminuir a duração do bloqueio, independentemente de suas permissões.

Um snapshot não pode ser excluído durante o período de desistência.

Se especificado, o período de desistência começará imediatamente após você bloquear o snapshot. Se omitido, o snapshot é bloqueado imediatamente no modo de conformidade, sem um período de desistência.

O período de desistência pode variar de 1 a 72 horas. Para bloquear um snapshot no modo de conformidade imediatamente, sem um período de desistência, não especifique um período de desistência na solicitação.

Estado do bloqueio

O bloqueio de um snapshot pode estar em um dos seguintes estados:

- `compliance-cooloff`: o snapshot foi bloqueado no modo de conformidade, mas ainda está dentro do período de desistência. O snapshot não pode ser excluído, mas pode ser desbloqueado, e as configurações de bloqueio podem ser modificadas por usuários com as permissões apropriadas.

- `governance`: o snapshot está bloqueado no modo de governança. O snapshot não pode ser excluído, mas pode ser desbloqueado, e as configurações de bloqueio podem ser modificadas por usuários com as permissões apropriadas.
- `compliance`: o snapshot está bloqueado no modo de conformidade sem um período de desistência ou o período de desistência expirou. O snapshot não pode ser desbloqueado nem excluído. A duração do bloqueio só pode ser aumentada por usuários com as permissões apropriadas.
- `expired`: o snapshot foi bloqueado no modo de conformidade ou de governança, mas o bloqueio expirou. O snapshot não está bloqueado e pode ser excluído.

Considerações sobre o bloqueio de snapshots do Amazon EBS

- Você só pode bloquear um snapshot se ele estiver no estado `pending` ou `completed`.
  - Se você bloquear um snapshot enquanto ele estiver no estado `pending` e bloqueá-lo por um período específico, o período de duração do bloqueio só começará quando o snapshot atingir o estado `completed`. O snapshot não pode ser excluído enquanto estiver no estado `pending`.
  - Se você bloquear um snapshot enquanto ele estiver no estado `pending` e a criação do snapshot falhar por qualquer motivo, o bloqueio será cancelado.
- Se você estender a duração do bloqueio de um snapshot bloqueado no modo de conformidade após o término do período de desistência, não poderá especificar outro período de desistência. Se você especificar um período de desistência, a solicitação falhará.
- Você pode bloquear snapshots arquivados. E você pode arquivar os snapshots bloqueados.
- Você pode bloquear os snapshots associados a uma AMI.
- Você pode cancelar o registro de uma AMI que tenha snapshots associados que estejam bloqueados.
- Você pode excluir a chave do KMS usada para criptografar um snapshot bloqueado.
- Recomendamos que você não bloqueie os instantâneos criados por AWS Backup. AWS Backup já garante que seus instantâneos não sejam excluídos antes que o período de retenção expire. Para adicionar uma camada adicional de segurança aos instantâneos gerenciados pelo AWS Backup, recomendamos que você use o AWS Backup Vault Lock. Para obter mais informações, consulte AWS Backup Vault Lock.
- Você não pode bloquear snapshots durante a criação ou durante o registro da AMI.
- Você não pode bloquear os snapshots locais do Amazon EBS no AWS Outposts.

- A única maneira de excluir um snapshot bloqueado no modo de conformidade antes que o bloqueio expire é fechar a conta associada AWS .

  Se você fechar sua AWS conta enquanto bloqueou os instantâneos, AWS suspenderá sua conta por 90 dias com os instantâneos intactos. Se você não reabrir sua conta dentro de 90 dias, AWS excluirá seus instantâneos, mesmo que estejam bloqueados.

Permissões necessárias para o bloqueio de snapshots do Amazon EBS

Por padrão, os usuários não têm permissão para trabalhar com snapshots bloqueados. Para permitir que os usuários usem snapshots bloqueados, você deve criar políticas do IAM que concedam permissão para usar recursos e ações de API específicos. Para obter mais informações, consulte Criar políticas do IAM no Guia do usuário do IAM.

Tópicos

Permissões obrigatórias

Para trabalhar com bloqueios de snapshots, os usuários precisam das permissões a seguir.

- `ec2:LockSnapshot`: para bloquear snapshots.
- `ec2:UnlockSnapshot`: para desbloquear snapshots.
- `ec2:DescribeLockedSnapshots`: para visualizar as configurações de bloqueio de snapshots.

O exemplo de política do IAM a seguir dá aos usuários permissão para bloquear e desbloquear snapshots, e para visualizar as configurações de bloqueio de snapshots. Isso inclui a permissão `ec2:DescribeSnapshots` para usuários do console. Se algumas permissões não forem necessárias, você poderá removê-las da política.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:LockSnapshot",
```

```
            "ec2:UnlockSnapshot",
            "ec2:DescribeLockedSnapshots",
            "ec2:DescribeSnapshots"
        ]
    }]
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Restringir o acesso com chaves de condição

Você pode usar chaves de condição para restringir como os usuários podem bloquear snapshots.

Tópicos

- ec2: SnapshotLockDuration
- ec2: CoolOffPeriod

ec2: SnapshotLockDuration

Você pode usar a chave de condição `ec2:SnapshotLockDuration` para restringir os usuários a durações de bloqueio específicas quando bloquearem snapshots.

O exemplo de política a seguir restringe os usuários a especificar uma duração de bloqueio entre `10` e `50` dias.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan" : {
          "ebs:SnapshotLockDuration" : 10
        }
        "NumericLessThan":{
          "ebs:SnapshotLockDuration": 50
        }
      }
    }
  ]
}
```

ec2: CoolOffPeriod

Você pode usar a chave de condição `ec2:CoolOffPeriod` para impedir que os usuários bloqueiem os snapshots no modo de conformidade sem um período de desistência.

O exemplo de política a seguir restringe os usuários a especificar um período de desistência de mais de `48` horas quando bloquearem snapshots no modo de conformidade.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan": {
          "ec2:CoolOffPeriod": 48
        }
      }
```

```
    }
  ]
}
```

Trabalhar com o bloqueio de snapshots do Amazon EBS

Use os procedimentos a seguir para trabalhar com o bloqueio de snapshots do Amazon EBS.

Tarefas

- Bloquear um snapshot
- Desbloquear um snapshot
- Atualizar as configurações de bloqueio de snapshots
- Visualizar as configurações de bloqueio de snapshots

Bloquear um snapshot

Você pode bloquear um snapshot que esteja no estado `pending` ou `completed`. Para ter mais informações, consulte Considerações sobre o bloqueio de snapshots do Amazon EBS.

Console

Para bloquear um snapshot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot a ser bloqueado e escolha Ações, Configurações de snapshot, Gerenciar bloqueio de snapshots.
4. Selecione Bloquear snapshot.
5. Para Modo de bloqueio, escolha Modo de governança ou Modo de conformidade. Para ter mais informações, consulte Modo de bloqueio.
6. Para Duração do bloqueio, use um dos seguintes procedimentos:
   - Para bloquear o snapshot por um período específico, escolha Bloquear snapshot por e insira o período em dias ou anos.
   - Para bloquear o snapshot até uma data e hora específica, escolha Bloquear snapshot até e depois selecione a data e hora de expiração.

Para ter mais informações, consulte Duração do bloqueio.

7. (Somente no modo de conformidade) Para Período de desistência, especifique um período de desistência durante o qual você poderá desbloquear o snapshot e modificar a configuração de bloqueio. Para ter mais informações, consulte Período de desistência.
8. (Somente no modo de conformidade) Para confirmar que você deseja bloquear o snapshot no modo de conformidade e que não poderá desbloqueá-lo após o término do período de desistência, escolha Confirmar.
9. Escolha Salvar configurações.

AWS CLI

Para bloquear um snapshot no modo de governança

Use o comando lock-snapshot da AWS CLI . Para `--snapshot-id`, especifique o ID do snapshot a ser bloqueado. Em `--lock-mode`, especifique `governance`. Para bloquear o snapshot por um período específico, em `--lock-duration`, especifique o período durante o qual o snapshot deverá ficar bloqueado. Ou, para bloquear o snapshot até uma data específica, em `--expiration-date`, especifique a data e hora em que o bloqueio deverá expirar, no fuso horário UTC (`YYYY-MM-DDThh:mm:ss.sssZ`).

```
$ aws ec2 lock-snapshot --snapshot-id snapshot_id \
 --lock-mode governance \
 --lock-duration 1-36500_days | --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

Para bloquear um snapshot no modo de conformidade

Use o comando lock-snapshot da AWS CLI . Para `--snapshot-id`, especifique o ID do snapshot a ser bloqueado. Em `--lock-mode`, especifique `compliance`. Para `--cool-off-period`, opcionalmente, especifique um período de desistência em horas. Para bloquear o snapshot por um período específico, em `--lock-duration`, especifique o período durante o qual o snapshot deverá ficar bloqueado. Ou, para bloquear o snapshot até uma data específica, em `--expiration-date`, especifique a data e hora em que o bloqueio deverá expirar, no fuso horário UTC (`YYYY-MM-DDThh:mm:ss.sssZ`).

```
$ aws ec2 lock-snapshot --snapshot-id snapshot_id \
 --lock-mode compliance \
```

```
--cool-off-period 1-72_hours \
--lock-duration 1-36500_days | --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

Desbloquear um snapshot

Você só pode desbloquear um snapshot se ele estiver bloqueado no modo de governança ou se estiver bloqueado no modo de conformidade e ainda estiver dentro do período de desistência.

Console

Para desbloquear um snapshot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot a ser desbloqueado e escolha Ações, Configurações de snapshot, Gerenciar bloqueio de snapshots.
4. Escolha Desbloquear snapshot e depois escolha Desbloquear snapshot novamente para confirmar.

AWS CLI

Para desbloquear um snapshot

Use o comando unlock-snapshot da AWS CLI . Para `--snapshot-id`, especifique o ID do snapshot a ser desbloqueado.

```
$ aws ec2 unlock-snapshot --snapshot-id snapshot_id
```

Atualizar as configurações de bloqueio de snapshots

As atualizações permitidas dependem do estado do bloqueio:

- `governance`: você pode alterar o modo de bloqueio, aumentar ou diminuir a duração do bloqueio e adiar ou antecipar a data de expiração.
- `compliance-cooloff`: você pode alterar o modo de bloqueio, aumentar ou diminuir o período de desistência, aumentar ou diminuir a duração do bloqueio e adiar ou antecipar a data de expiração.
- `compliance`: você só pode aumentar a duração do bloqueio ou a data de expiração.

Console

Para atualizar as configurações de bloqueio de snapshots

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot cujas configurações de bloqueio serão modificadas e escolha Ações, Configurações de snapshot, Gerenciar bloqueio de snapshots.
4. Atualize as configurações conforme necessário e escolha Salvar configurações de bloqueio.

AWS CLI

Para atualizar as configurações de bloqueio de snapshots

Use o comando lock-snapshot da AWS CLI . Para `--snapshot-id`, especifique o ID do snapshot cujas configurações de bloqueio serão atualizadas. Depois, especifique somente as opções a serem modificadas.

Visualizar as configurações de bloqueio de snapshots

Use um dos métodos a seguir para visualizar as configurações de bloqueio de um snapshot.

Console

Para visualizar as configurações de bloqueio de snapshots

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot cujas configurações de bloqueio devem ser visualizadas e escolha Ações, Configurações de snapshot, Gerenciar bloqueio de snapshots.

AWS CLI

Para visualizar as configurações de bloqueio de snapshots

Use o comando describe-locked-snapshots. AWS CLI Para `--snapshot-ids`, especifique os IDs dos snapshots cujas configurações de bloqueio serão visualizadas.

```
$ aws ec2 describe-locked-snapshots --snapshot-ids snapshot_id
```

Monitore bloqueios de snapshots do Amazon EBS usando AWS CloudTrail

Você pode monitorar as chamadas de API para bloqueio de snapshots como eventos, incluindo as chamadas feitas do console e chamadas de código para APIs. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações, consulte Registrar chamadas de API em log usando o AWS CloudTrail.

Monitore bloqueios de snapshots do Amazon EBS usando a Amazon EventBridge

O Amazon EBS emite eventos relacionados a ações de bloqueio de snapshots. Você pode usar AWS Lambda a Amazon EventBridge para lidar com notificações de eventos de forma programática. Os eventos são emitidos com base no melhor esforço. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

Os seguintes eventos são emitidos:

- Snapshot bloqueado com sucesso no modo de governança ou de conformidade.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "source": 012345678901,
    "lockState": "compliance-cooloff",
```

```
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- Evento de falha de bloqueio quando um snapshot é bloqueado enquanto está no estado `pending` e não consegue passar para o estado `completed`.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "failed",
    "cause": "snapshot failed",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "pending-compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- Bloqueio expirado

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
```

```
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockDurationExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "expired",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123
  }
}
```

- O período de desistência expirou após ser bloqueado no modo de conformidade.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "cooloffperiodExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
```

```
}
```

Bloquear o acesso público aos snapshots

Para evitar o compartilhamento público dos snapshots, você pode habilitar o bloqueio do acesso público aos snapshots. Depois de habilitar o bloqueio do acesso público aos snapshots em uma região, qualquer tentativa de compartilhar publicamente os snapshots nessa região será automaticamente bloqueada. Isso pode ajudar você a melhorar a segurança dos snapshots e a proteger os dados dos snapshots contra acesso não autorizado ou não intencional.

O bloqueio do acesso público aos snapshots pode ser habilitado de um de dois modos:

- Bloquear todos os compartilhamentos: bloqueia todos os compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Além disso, os snapshots que já foram compartilhados publicamente são tratados como privados e não estão mais disponíveis publicamente.
- Bloquear novos compartilhamentos: bloqueia apenas os novos compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Porém, os snapshots que já foram compartilhados publicamente permanecem disponíveis publicamente.

Definição de preço

O bloqueio do acesso público aos snapshots pode ser habilitado sem nenhum custo adicional.

Sumário

Considerações

- Bloquear o acesso público aos snapshots não impede o compartilhamento de snapshots privados.
- Se você habilitar o bloqueio do acesso público aos snapshots no modo de bloquear todos os compartilhamentos, isso não alterará as permissões para os snapshots que já foram compartilhados publicamente. Em vez disso, evitará que esses snapshots fiquem visíveis e acessíveis ao público. Portanto, os atributos desses snapshots continuam indicando que eles são compartilhados publicamente, embora não estejam disponíveis publicamente.
- Se o bloqueio do acesso público aos snapshots estiver habilitado no modo de bloquear todos os compartilhamentos e você alterar o modo para bloquear novos compartilhamentos ou desabilitar o bloqueio do acesso público, todos os snapshots que foram compartilhados publicamente antes não serão mais tratados como privados e voltarão a ser acessíveis ao público.
- Bloquear o acesso público a snapshots é uma configuração regional. Ela se aplica a todos os snapshots na região em que é habilitada. Você precisa habilitar o bloqueio do acesso público a snapshots em toda região na qual deseja evitar o compartilhamento público dos snapshots.
- Bloquear o acesso público é uma configuração no nível da conta. Ela se aplica a todos os usuários da conta, incluindo os usuários administradores. Você não pode habilitar o bloqueio de acesso público aos snapshots no nível da organização.
- Bloquear o acesso público aos snapshots não evita o compartilhamento público das AMIs baseadas no EBS. Se você habilitar o bloqueio do acesso público aos snapshots, os usuários continuarão podendo compartilhar publicamente as AMIs baseadas no EBS. Se uma AMI baseada no EBS for compartilhada publicamente, os usuários com acesso a essa AMI poderão criar volumes a partir dos snapshots a ela associados. Para evitar o compartilhamento público das AMIs, é possível habilitar o bloqueio de acesso público às AMIs.
- O bloqueio do acesso público para instantâneos não é suportado com os instantâneos locais ativados. AWS Outposts

Permissões do IAM

Por padrão, os usuários não têm permissão para trabalhar com o bloqueio de acesso público aos snapshots. Para permitir que os usuários trabalhem com o bloqueio de acesso público aos snapshots, você deve criar políticas do IAM que concedam permissão para usar ações de API específicas. Depois que as políticas forem criadas, você deverá adicionar as permissões aos seus usuários, grupos ou perfis.

Para trabalhar com o bloqueio de snapshots, os usuários precisam das permissões a seguir.

- `ec2:EnableSnapshotBlockPublicAccess`: habilitar o bloqueio do acesso público aos snapshots e modificar o modo.
- `ec2:DisableSnapshotBlockPublicAccess`: desabilitar o bloqueio do acesso público aos snapshots.
- `ec2:GetSnapshotBlockPublicAccessState`: visualizar o bloqueio do acesso público aos snapshots é uma configuração para uma região.

A seguir está um exemplo de política do IAM. Se algumas permissões não forem necessárias, você poderá removê-las da política.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:EnableSnapshotBlockPublicAccess",
            "ec2:DisableSnapshotBlockPublicAccess",
            "ec2:GetSnapshotBlockPublicAccessState"
        ],
        "Resource": "*"
    }]
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.

- (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Habilitar o bloqueio do acesso público aos snapshots

Use os procedimentos a seguir para configurar e monitorar o bloqueio do acesso público aos snapshots.

Tarefas

- Configurar o bloqueio do acesso público aos snapshots
- Visualizar a configuração de acesso público aos snapshots
- Desabilitar o bloqueio do acesso público aos snapshots

Configurar o bloqueio do acesso público aos snapshots

Habilite o bloqueio do acesso público aos snapshots para evitar o compartilhamento público de snapshots na região. Depois que esse atributo é habilitado, as solicitações para compartilhar publicamente snapshots na região são bloqueadas.

> **Important**
>
> Se o bloqueio do acesso público aos snapshots estiver habilitado no modo de bloquear todos os compartilhamentos e você alterar o modo para bloquear novos compartilhamentos, todos os snapshots que foram compartilhados publicamente antes não serão mais tratados como privados e voltarão a ser acessíveis ao público.

Console

Para configurar o bloqueio do acesso público aos snapshots

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Painel do EC2 e depois, em Atributos da conta (do lado direito), escolha Proteção e segurança de dados.
3. Na seção Bloquear o acesso público aos snapshots do EBS, escolha Gerenciar.

4. Selecione Bloquear acesso público e depois escolha uma das seguintes opções:
   - Bloquear todos os compartilhamentos: para bloquear todos os compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Além disso, os snapshots que já foram compartilhados publicamente são tratados como privados e não estão mais disponíveis publicamente.
   - Bloquear novos compartilhamentos públicos: para bloquear apenas novos compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Porém, os snapshots que já foram compartilhados publicamente permanecem disponíveis publicamente.
5. Escolha Atualizar.

AWS CLI

Para habilitar ou modificar o bloqueio do acesso público aos snapshots

Use o comando enable-snapshot-block-public-access. Para `--state`, especifique um dos seguintes valores:

- `block-all-sharing`: para bloquear todos os compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Além disso, os snapshots que já foram compartilhados publicamente são tratados como privados e não estão mais disponíveis publicamente.
- `block-new-sharing`: para bloquear apenas novos compartilhamentos públicos dos snapshots. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Porém, os snapshots que já foram compartilhados publicamente permanecem disponíveis publicamente.

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

Visualizar a configuração de acesso público aos snapshots

O bloqueio do acesso público pode estar em um dos seguintes estados para cada região da sua conta.

- Bloquear todos os compartilhamentos: todos os compartilhamentos públicos dos snapshots são bloqueados. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Além disso, os snapshots que já foram compartilhados publicamente são tratados como privados e não estão mais disponíveis publicamente.
- Bloquear novos compartilhamentos: somente novos compartilhamentos públicos dos snapshots são bloqueados. Os usuários da conta não podem solicitar novos compartilhamentos públicos. Porém, os snapshots que já foram compartilhados publicamente permanecem disponíveis publicamente.
- Desbloqueado: o compartilhamento público não é bloqueado. Os usuários podem compartilhar snapshots publicamente.

Console

Para visualizar a configuração de bloqueio do acesso público aos snapshots

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Painel do EC2 e depois, em Atributos da conta (do lado direito), escolha Proteção e segurança de dados.
3. A seção Bloquear o acesso público aos snapshots do EBS mostra a configuração atual.

AWS CLI

Para visualizar a configuração de bloqueio do acesso público aos snapshots

Use o comando get-snapshot-block-public-access-state.

```
aws ec2 get-snapshot-block-public-access-state
```

Desabilitar o bloqueio do acesso público aos snapshots

Desabilite bloqueio do acesso público aos snapshots para permitir o compartilhamento público dos snapshots na região. Depois que esse atributo é desabilitado, os usuários podem compartilhar publicamente os snapshots na região.

> **Important**
>
> Se o bloqueio do acesso público aos snapshots estiver habilitado no modo de bloquear todos os compartilhamentos e você desabilitar o bloqueio do acesso público, todos os snapshots que foram compartilhados publicamente antes deixarão de ser tratados como privados e se tornarão acessíveis ao público novamente.

Console

Para desabilitar o bloqueio do acesso público aos snapshots

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Painel do EC2 e depois, em Atributos da conta (do lado direito), escolha Proteção e segurança de dados.
3. Na seção Bloquear o acesso público aos snapshots do EBS, escolha Gerenciar.
4. Desmarque Bloquear o acesso público e selecione Salvar.

AWS CLI

Para desabilitar o bloqueio do acesso público aos snapshots

Use o comando disable-snapshot-block-public-access.

```
aws ec2 disable-snapshot-block-public-access
```

Monitore, bloqueie o acesso público para snapshots usando a Amazon EventBridge

O Amazon EBS emite eventos relacionados ao bloqueio do acesso público aos snapshots. Você pode usar AWS Lambda a Amazon EventBridge para lidar com notificações de eventos de forma programática. Os eventos são emitidos com base no melhor esforço. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

Os seguintes eventos são emitidos:

- Habilitar o bloqueio do acesso público aos snapshots no modo de bloquear todos os compartilhamentos públicos

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-all-sharing",
    "message": "Block Public Access was successfully enabled in 'block-all-sharing'
 mode"
  }
}
```

- Habilitar o bloqueio do acesso público aos snapshots no modo de bloquear novos compartilhamentos

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-new-sharing",
    "message": "Block Public Access was successfully enabled in 'block-new-sharing'
 mode"
  }
}
```

- Desabilitar o bloqueio do acesso público aos snapshots

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Disabled",
  "source": "aws.ec2",
```

```
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "unblocked",
    "message": "Block Public Access was successfully disabled"
  }
}
```

Lixeira de snapshots

A Recycle Bin (Lixeira) é um recurso de recuperação de dados que permite restaurar snapshots do Amazon EBS e AMIs apoiadas pelo EBS excluídos acidentalmente. Ao usar a Recycle Bin (Lixeira), se seus recursos forem excluídos, eles serão retidos na Recycle Bin (Lixeira) por um período de tempo que você especifica antes de serem excluídos permanentemente.

É possível restaurar um recurso da Recycle Bin (Lixeira) a qualquer momento antes que o período de retenção expire. Depois que um recurso é restaurado da Recycle Bin (Lixeira), ele é removido da Recycle Bin (Lixeira) e é possível usá-lo como usa qualquer outro recurso do mesmo tipo em sua conta. Se o período de retenção expirar e o recurso não for restaurado, ele será excluído permanentemente da Recycle Bin (Lixeira) e não estará mais disponível para recuperação.

Os snapshots na lixeira são cobrados à mesma taxa que os snapshots comuns em sua conta. Não há encargos adicionais pelo uso da lixeira e de regras de retenção. Para obter mais informações, consulte Definição de preço do Amazon EBS.

Para obter mais informações, consulte Lixeira.

Tópicos

- Permissões para trabalhar com snapshots na lixeira
- Exibir snapshots na lixeira
- Restaurar os snapshots da lixeira

Permissões para trabalhar com snapshots na lixeira

Por padrão, os usuários do IAM não têm permissão para trabalhar com os snapshots que estão na Lixeira. Para permitir que os usuários trabalhem com esses recursos, você deve criar políticas do

IAM que concedam permissão para o uso de recursos e ações de API específicos. Depois que as políticas forem criadas, você deverá adicionar as permissões aos seus usuários, grupos ou perfis.

Para visualizar e recuperar snapshots que estão na Lixeira, os usuários precisam ter as seguintes permissões:

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Para gerenciar etiquetas para snapshots na Lixeira, os usuários precisam das permissões adicionais a seguir.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Para usar o console da Lixeira, os usuários precisam ter a permissão `ec2:DescribeTags`.

A seguir está um exemplo de política do IAM. Ela inclui a permissão `ec2:DescribeTags` para usuários do console e inclui as permissões `ec2:CreateTags` e `ec2:DeleteTags` para gerenciar etiquetas. Se não forem necessárias permissões, será possível removê-las da política.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListSnapshotsInRecycleBin",
            "ec2:RestoreSnapshotFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
```

```
      },

    ]
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Para obter mais informações sobre as permissões necessárias para usar a Lixeira, consulte Permissões do IAM necessárias.

Exibir snapshots na lixeira

Enquanto um snapshot estiver na lixeira, é possível visualizar informações limitadas sobre ele, incluindo:

- O ID do snapshot.
- A descrição do snapshot.
- O ID do volume do qual o snapshot foi criado.
- A data e a hora em que o snapshot foi excluído e entrou na lixeira.
- A data e a hora em que o período de retenção expira. O snapshot será excluído permanentemente da lixeira nessa hora.

É possível visualizar os snapshots na lixeira usando um dos métodos a seguir.

Recycle Bin console

Para visualizar os snapshots na lixeira usando o console

1. Abra o console da Lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Recycle Bin (Lixeira).
3. A grade lista todos os snapshots que estão atualmente na lixeira. Para visualizar os detalhes de um snapshot específico, selecione-o na grade e escolha Actions (Ações), View details (Exibir detalhes).

AWS CLI

Para visualizar instantâneos na Lixeira usando o AWS CLI

Use o AWS CLI comando list-snapshots-in-recycle-bin. Inclua a opção `--snapshot-id` para visualizar um snapshot específico. Ou omita a opção `--snapshot-id` para visualizar todos os snapshots na lixeira.

```
$ C:\> aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Por exemplo, o comando a seguir retorna informações sobre o snapshot `snap-01234567890abcdef` na lixeira.

```
$ C:\> aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Resultado do exemplo:

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
```

```
}
```

Restaurar os snapshots da lixeira

Você não pode usar um snapshot de nenhum modo enquanto ele está na lixeira. Para usar o snapshot, é necessário primeiro restaurá-lo. Quando você restaura um snapshot da lixeira, ele fica imediatamente disponível para uso e é removido da lixeira. É possível usar um snapshot restaurado como usa qualquer outro snapshot em sua conta.

É possível restaurar um snapshot da lixeira usando um dos métodos a seguir.

Recycle Bin console

Para restaurar um snapshot da lixeira usando o console

1. Abra o console da Lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Recycle Bin (Lixeira).
3. A grade lista todos os snapshots que estão atualmente na lixeira. Selecione o snapshot a ser restaurado e escolha Recover (Recuperar).
4. Quando solicitado, escolha Recover (Recuperar).

AWS CLI

Para restaurar um instantâneo excluído da Lixeira usando o AWS CLI

Use o AWS CLI comando restore-snapshot-from-recycle-bin. Em `--snapshot-id`, especifique o ID do snapshot a ser restaurado.

```
$ C:\> aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Por exemplo, o comando a seguir restaura o snapshot `snap-01234567890abcdef` da lixeira.

```
$ C:\> aws ec2 restore-snapshot-from-recycle-bin --snapshot-id
 snap-01234567890abcdef
```

Resultado do exemplo:

```
{
```

```
    "SnapshotId": "snap-01234567890abcdef",
    "Description": "Monthly data backup snapshot",
    "Encrypted": false,
    "OwnerId": "111122223333",
    "Progress": "100%",
    "StartTime": "2021-12-01T13:00:00.000000+00:00",
    "State": "recovering",
    "VolumeId": "vol-ffffffff",
    "VolumeSize": 30
}
```

Amazon EBS local snapshots on Outposts

Os snapshots do Amazon EBS são uma cópia point-in-time dos volumes do EBS.

Por padrão, os snapshots de volumes do EBS em um Outpost são armazenados no Amazon S3, na região do Outpost. Também é possível usar Snapshots locais do Amazon EBS em Outposts para armazenar snapshots de volumes em um Outpost localmente no Amazon S3 no próprio Outpost. Isso garante que os dados do snapshot permaneçam no Outpost e no seu local. Além disso, é possível usar políticas e permissões do AWS Identity and Access Management (IAM) para configurar políticas de imposição de residência de dados para garantir que os dados de snapshots não saiam do Outpost. Isso é especialmente útil se você mora em um país ou região que ainda não foi atendida por uma região da AWS e que apresente requisitos de residência de dados.

Este tópico fornece informações sobre como trabalhar com Snapshots locais do Amazon EBS em Outposts. Para obter mais informações sobre os snapshots do Amazon EBS e sobre como trabalhar com snapshots em uma região da AWS, consulte Snapshots do Amazon EBS.

Para obter mais informações sobre AWS Outposts, consulte AWS Outposts Features (Recursos) e o Guia do Usuário do AWS Outposts. Para obter informações sobre preços, consulte Preços do AWS Outposts.

Tópicos

Perguntas frequentes

1. O que são snapshots locais?

   Por padrão, os snapshots de volumes do Amazon EBS em um Outpost são armazenados no Amazon S3, na região do Outpost. Se o Outpost estiver provisionado com o Amazon S3 on Outposts, é possível optar por armazenar os snapshots localmente no próprio Outpost. Os snapshots locais são incrementais, o que significa que serão salvos somente os blocos no volume que mudaram após o snapshot mais recente. É possível usar esses snapshots para restaurar a qualquer momento um volume no mesmo Outpost que o snapshot. Para obter mais informações sobre snapshots do Amazon EBS, consulte Snapshots do Amazon EBS.

2. Por que devo usar snapshots locais?

   Os snapshots são uma maneira conveniente de fazer backup de seus dados. Com snapshots locais, todos os seus dados de snapshots são armazenados localmente no Outpost. Isso significa que ele não deixa o seu local. Isso será útil principalmente se você mora em um país ou região que ainda não está atendida por uma região da AWS e que apresente requisitos de residência.

   Além disso, o uso de snapshots locais pode ajudar a reduzir a largura de banda usada para a comunicação entre a região e o Outpost em ambientes restritos pela largura de banda.

3. Como faço para impor a residência de dados de snapshots em Outposts?

   É possível usar políticas do AWS Identity and Access Management (IAM) para controlar as permissões que os principais (contas da AWS, usuários do IAM e funções do IAM) têm ao trabalhar com snapshots locais para impor a residência de dados. É possível criar uma política que evite que as entidades criem snapshots a partir de volumes e instâncias do Outpost e armazenem os snapshots em uma região da AWS. No momento, não há suporte para copiar snapshots e imagens de um Outpost para uma região. Para obter mais informações, consulte Controlar o acesso com o IAM.

4. Há suporte para snapshots locais multivolume e consistentes com falhas?

   Sim, é possível criar snapshots locais multivolume e consistentes com falhas em instâncias em um Outpost.

5. Como crio snapshots locais?

   É possível criar snapshots manualmente usando a AWS Command Line Interface (AWS CLI) ou o console do Amazon EC2. Para obter mais informações, consulte Trabalhe com snapshots locais.

Também é possível automatizar o ciclo de vida de snapshots locais por meio do Amazon Data Lifecycle Manager. Para obter mais informações, consulte Automatize snapshots em um Outpost.

6. Posso criar, usar ou excluir snapshots locais se meu Outpost perder a conectividade com a sua região?

Não. O Outpost deve ter conectividade com a região dele, pois ela fornece serviços de acesso, autorização, registro em log e monitoramento, que são essenciais para a integridade de seus snapshots. Se não houver conectividade, você não poderá criar novos snapshots locais, criar volumes, executar instâncias a partir de snapshots locais existentes ou excluir snapshots locais.

7. O quão rápido a capacidade de armazenamento do Amazon S3 fica disponível após a exclusão de snapshots locais?

A capacidade de armazenamento do Amazon S3 fica disponível dentro de 72 horas após a exclusão de snapshots locais e de volumes que fazem referência a eles.

8. Como posso garantir que a capacidade do Amazon S3 não se esgote no meu Outpost?

Recomendamos que você use alarmes Amazon CloudWatch para monitorar a sua capacidade de armazenamento do Amazon S3 e exclua snapshots e volumes de que não precisa mais; assim você previne o fim da capacidade de armazenamento. Se você estiver usando o Amazon Data Lifecycle Manager para automatizar o ciclo de vida de snapshots locais, certifique-se de que as suas políticas de retenção de snapshots não retenham snapshots por mais tempo do que o necessário.

9. O que acontece se eu ficar sem capacidade local do Amazon S3 nos Outposts?

Se você ficar sem capacidade local do Amazon S3 em seus Outposts, o Amazon Data Lifecycle Manager não poderá criar snapshots locais com êxito nos Outposts. O Amazon Data Lifecycle Manager tentará criar os snapshots locais nos Outposts, mas os snapshots passarão imediatamente para o estado de `error` e serão excluídos pelo Amazon Data Lifecycle Manager. Recomendamos que você use a métrica `SnapshotsCreateFailed` do Amazon CloudWatch para monitorar as políticas de ciclo de vida do snapshot e detectar falhas na criação de snapshots. Para ter mais informações, consulte Monitore suas políticas usando a Amazon CloudWatch.

10. Posso usar snapshots locais e AMIs baseadas em snapshots locais com instâncias spot e uma frota spot?

Não, você não pode usar snapshots locais ou AMIs baseadas em snapshots locais para executar instâncias spot ou uma frota spot.

11. Posso usar snapshots locais e AMIs baseadas em snapshots locais com o Amazon EC2 Auto Scaling?

Sim, é possível usar snapshots locais e AMIs baseadas em snapshots locais para iniciar grupos de Auto Scaling em uma sub-rede que esteja no mesmo Outpost que os snapshots. A função vinculada a serviços do grupo Amazon EC2 Auto Scaling deve ter permissão para usar a Chave do KMS usada para criptografar os snapshots.

Você não pode usar snapshots locais ou AMIs compatíveis com snapshots locais para iniciar grupos do Auto Scaling em uma região da AWS.

Pré-requisitos

Para armazenar snapshots em um Outpost, é necessário ter um Outpost provisionado com o Amazon S3 em Outposts. Para mais informações sobre o Amazon S3 no Outposts, consulte Usar o Amazon S3 no Outposts no Guia do usuário do Amazon Simple Storage Service.

Considerações

Ao trabalhar com snapshots locais, lembre-se do seguinte:

- O Outposts deve ter conectividade em sua região da AWS para usar snapshots locais.
- Os metadados do snapshot são armazenados na região da AWS associada ao Outpost. Isso não inclui nenhum dado de snapshot.
- Os snapshots armazenados em Outposts são criptografados por padrão. Não há suporte para snapshots não criptografados. Os snapshots criados em um Outpost e snapshots copiados para um Outpost são criptografados usando a Chave do KMS de criptografia padrão para a região ou uma Chave do KMS diferente que você especificar ao fazer a solicitação.
- Ao criar um volume em um Outpost a partir de um snapshot local, você não pode criptografar o volume novamente usando uma Chave do KMS de criptografia diferente. Os volumes criados de snapshots locais devem ser criptografados usando a mesma Chave do KMS que o snapshot de origem.
- Depois que você excluir snapshots locais de um Outpost, a capacidade de armazenamento do Amazon S3 usada pelos snapshots excluídos fica disponível por 72 horas. Para ter mais informações, consulte Exclua snapshots locais.
- Você não pode exportar snapshots locais de um Outpost.

- Você não pode habilitar a restauração rápida de snapshots para snapshots locais.
- APIs diretas do EBS não são compatíveis com snapshots locais.
- Não é possível copiar snapshots locais ou AMIs de um Outpost para uma região da AWS, de um Outpost para outro ou dentro de um Outpost. No entanto, é possível copiar snapshots de uma região da AWS para um Outpost. Para obter mais informações, consulte Copiar snapshots de uma região da AWS para um Outpost.
- Ao copiar um snapshot de uma região da AWS para um Outpost, os dados são transferidos pelo link do serviço. Copiar vários snapshots simultaneamente pode afetar outros serviços em execução no Outpost.
- Você não pode compartilhar snapshots locais.
- Use as políticas do IAM para garantir que seus requisitos de residência de dados sejam cumpridos. Para obter mais informações, consulte Controlar o acesso com o IAM.
- Os Snapshots locais são backups incrementais. Serão salvos somente os blocos no volume que foram alterados depois do seu snapshot mais recente. Cada snapshot local contém todas as informações necessárias para restaurar os seus dados (desde o momento em que o snapshot foi capturado) até um volume novo do EBS. Para obter mais informações, consulte Como funcionam os snapshots.
- Você não pode usar políticas do IAM para impor a residência de dados para as ações CopySnapshot (Copiar snapshot) e CopyImage (Copiar imagem).

Controlar o acesso com o IAM

É possível usar políticas do AWS Identity and Access Management (IAM) para controlar as permissões que os principais (contas da AWS, usuários do IAM e funções do IAM) têm ao trabalhar com snapshots locais. Veja a seguir as políticas de exemplo que é possível usar para conceder ou negar permissão para executar ações específicas com snapshots locais.

> **Important**
>
> No momento, não há suporte para copiar snapshots e imagens de um Outpost para uma região. Como resultado, você não pode usar as políticas do IAM para impor a residência de dados para as ações CopySnapshot (Copiar snapshot) e CopyImage (Copiar imagem).

Tópicos

- Imponha a residência de dados para snapshots
- Impeça que as entidades excluam snapshots locais

Imponha a residência de dados para snapshots

A política de exemplo a seguir impede que todas as entidades criem snapshots de volumes e instâncias no Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef` e armazenem os dados de snapshot em uma região da AWS. As entidades ainda podem criar snapshots locais. Essa política garante que todos os snapshots permaneçam no Outpost.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:SourceOutpostArn": "arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0"
                },
                "Null": {
                    "ec2:OutpostArn": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Impeça que as entidades excluam snapshots locais

A política de exemplo a seguir impede que todos as entidades excluam snapshots locais armazenados no Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:OutpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

Trabalhe com snapshots locais

As seções a seguir explicam como usar snapshots locais.

Tópicos

- Regras para armazenar snapshots
- Crie snapshots locais a partir de volumes em um Outpost
- Crie snapshots locais multivolume a partir de instâncias em um Outpost

- Crie AMIs em snapshots locais
- Copiar snapshots de uma região da AWS para um Outpost
- Copiar AMIs de uma região da AWS para um Outpost
- Crie volumes a partir de snapshots locais
- Execute instâncias a partir de AMIs baseadas em snapshots locais
- Exclua snapshots locais
- Automatize snapshots em um Outpost

Regras para armazenar snapshots

As regras a seguir se aplicam ao armazenamento de snapshots:

- Se o snapshot mais recente de um volume for armazenado em um Outpost, todos os snapshots sucessivos deverão ser armazenados no mesmo Outpost.
- Se o snapshot mais recente de um volume for armazenado em uma região da AWS, todos os snapshots sucessivos deverão ser armazenados na mesma região. Para começar a criar snapshots locais a partir desse volume, faça o seguinte:

  1. Crie um snapshot do volume na região da AWS.
  2. Copie o snapshot para o Outpost da região da AWS.
  3. Crie um novo volume a partir do snapshot local.
  4. Anexe o volume a uma instância no Outpost.

  Para o novo volume no Outpost, o próximo snapshot pode ser armazenado no Outpost ou na região da AWS. Todos os snapshots sucessivos deverão ser armazenados nessa mesma localização.
- Os snapshots locais, incluindo snapshots criados em um Outpost e snapshots copiados para um Outpost de uma região da AWS, só podem ser usados para criar volumes no mesmo Outpost.
- Se você criar um volume em um Outpost a partir de um snapshot em uma região, todos os snapshots sucessivos desse novo volume deverão ficar na mesma região.
- Se você criar um volume em um Outpost de um snapshot local, todos os snapshots sucessivos desse novo volume deverão estar no mesmo Outpost.

Crie snapshots locais a partir de volumes em um Outpost

É possível criar snapshots locais a partir de volumes no seu Outpost. É possível optar por armazenar os snapshots no mesmo Outpost que o volume de origem ou na região do Outpost.

Os Snapshots locais podem ser usados para criar volumes somente no mesmo Outpost.

É possível criar snapshots locais a partir de volumes em um Outpost usando um dos métodos a seguir.

Console

Para criar snapshots locais a partir de volumes em um Outpost

Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

1. No painel de navegação, escolha Volumes.
2. Selecione o volume no Outpost e escolha Actions (Ações) e Create snapshot (Criar snapshot).
3. (Opcional) Em Description (Descrição), insira uma breve descrição para o snapshot.
4. Em Snapshot destination Destino do snapshot), escolha AWS Outpost. O snapshot será criado no mesmo Outpost que o volume de origem. O campo Outpost ARN (ARN do Outpost) exibe o nome de recurso da Amazon (ARN) do Outpost de destino.
5. (Opcional) Escolha Add Tag (Adicionar tag) para adicionar tags ao seu snapshot. Para cada tag, forneça uma chave e um valor.
6. Escolha Create Snapshot (Criar snapshot).

Command line

Para criar snapshots locais a partir de volumes em um Outpost

Use o comando create-snapshot (Criar snapshot). Especifique o ID do volume a partir do qual deseja criar o snapshot e o ARN do Outpost de destino em que deseja armazenar o snapshot. Se você omitir o ARN do Outpost, o snapshot será armazenado na região da AWS do Outpost.

Por exemplo, o comando a seguir cria um snapshot local de volume `vol-1234567890abcdef0` e armazena o snapshot no Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --outpost-arn
 arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0 --description
 "single volume local snapshot"
```

Crie snapshots locais multivolume a partir de instâncias em um Outpost

É possível criar snapshots locais multivolume e consistentes com falhas em instâncias no seu Outpost. É possível optar por armazenar os snapshots no mesmo Outpost que a instância de origem ou na região do Outpost.

Os snapshots locais multivolume podem ser usados para criar volumes somente no mesmo Outpost.

É possível criar snapshots locais multivolume a partir de instâncias em um Outpost usando um dos métodos a seguir.

Console

Para criar snapshots locais multivolume a partir de instâncias em um Outpost

Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

1. No painel de navegação, selecione Snapshots.
2. Escolha Create Snapshot (Criar snapshot).
3. Em Select resource type (Selecionar tipo de recurso), escolha Instance (Instância).
4. Em Instance ID (ID de instância), selecione a instância no Outpost a partir da qual deseja criar os snapshots.
5. (Opcional) Em Description (Descrição), insira uma breve descrição para os snapshots.
6. Em Snapshot destination Destino do snapshot), escolha AWS Outpost. Os snapshots serão criados no mesmo Outpost que a instância de origem. O Outpost ARN (ARN do Outpost) exibe o ARN do Outpost de destino.
7. Para excluir o volume raiz da instância do conjunto de snapshots de vários volumes, selecione Exclude root volume (Excluir volume raiz). Ao fazer isso, o Amazon EBS não criará um snapshot do volume raiz da instância.
8. Para excluir volumes de dados específicos do conjunto de snapshots de vários volumes, selecione Exclude specific data volumes (Excluir volumes de dados específicos). A seção Attached data volumes (Volumes de dados anexados) lista todos os volumes de dados que atualmente estão anexados à instância selecionada.

Na seção Attached data volumes (Volumes de dados anexados), desmarque os volumes de dados a serem excluídos do conjunto de snapshots de vários volumes. Somente os volumes que forem selecionados serão incluídos no conjunto de snapshots de vários volumes.

9. (Opcional) Para copiar automaticamente as etiquetas dos volumes de origem para os snapshots correspondentes, para Copy tags from source volume (Copiar etiquetas do volume de origem), selecione Copy tags (Copiar etiquetas). Isso define os metadados do snapshot, como políticas de acesso, informações de anexo e alocação de custos, para corresponderem com o volume de origem.
10. (Opcional) Para atribuir outras etiquetas personalizadas a snapshots, na seção Tags (Etiquetas), escolha Add tag (Adicionar etiqueta) e insira o par chave-valor. É possível adicionar até 50 tags.
11. Escolha Create Snapshot (Criar snapshot).

    Durante a criação do snapshot, os snapshots são gerenciados juntos. Se houver falha em um dos snapshots do conjunto de volumes, os outros snapshots no conjunto ficarão com o status de erro.

Command line

Para criar snapshots locais multivolume a partir de instâncias em um Outpost

Use o comando create-snapshots (Criar snapshots). Especifique o ID da instância a partir da qual deseja criar os snapshots e o ARN do Outpost de destino em que deseja armazenar os snapshots. Se você omitir o ARN do Outpost, os snapshots serão armazenados na região da AWS do Outpost.

Por exemplo, o comando a seguir cria snapshots dos volumes anexados à instância `i-1234567890abcdef0` e armazena os snapshots no Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 create-snapshots --instance-specification InstanceId=i-1234567890abcdef0
 --outpost-arn arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0
 --description "multi-volume local snapshots"
```

Crie AMIs em snapshots locais

É possível criar Imagens de máquina da Amazon (AMIs) usando uma combinação de snapshots locais e snapshots armazenados na região do Outpost. Por exemplo, se tiver um Outpost na região `us-east-1`, será possível criar uma AMI com volumes de dados que são baseados em snapshots locais nesse Outpost e um volume raiz que é baseado em um snapshot na região `us-east-1`.

> **Note**
>
> - Não é possível criar AMIs que incluam snapshots de base armazenados em vários Outposts.
> - No momento, você não pode criar AMIs diretamente de instâncias em Outposts usando a API CreateImage (Criar imagem) ou o console do Amazon EC2 para Outposts habilitados ao Amazon S3 em Outposts.
> - As AMIs baseadas em snapshots locais podem ser usadas para executar instâncias somente no mesmo Outpost.

Para criar uma AMI em um Outpost a partir de snapshots em uma região

1. Copie os snapshots da região para o Outpost. Para obter mais informações, consulte Copiar snapshots de uma região da AWS para um Outpost.
2. Use o console do Amazon EC2 ou o comando register-image (Registrar imagem) para criar a AMI usando as cópias de snapshots no Outpost. Para obter mais informações, consulte Creating an AMI from a snapshot (Como criar uma AMI a partir de um snapshot).

Para criar uma AMI em um Outpost a partir de uma instância em um Outpost

1. Crie snapshots a partir da instância no Outpost e armazene os snapshots no Outpost. Para obter mais informações, consulte Crie snapshots locais multivolume a partir de instâncias em um Outpost.
2. Use o console do Amazon EC2 ou o comando register-image (Registrar imagem) para criar a AMI usando os snapshots locais. Para obter mais informações, consulte Creating an AMI from a snapshot (Como criar uma AMI a partir de um snapshot).

Para criar uma AMI em uma região a partir de uma instância em um Outpost

1. Crie snapshots a partir da instância no Outpost e armazene-os na região. Para obter mais informações, consulte Crie snapshots locais a partir de volumes em um Outpost ou Crie snapshots locais multivolume a partir de instâncias em um Outpost.
2. Use o console do Amazon EC2 ou o comando register-image para criar a AMI usando as cópias de snapshot na região. Para obter mais informações, consulte Creating an AMI from a snapshot (Como criar uma AMI a partir de um snapshot).

Copiar snapshots de uma região da AWS para um Outpost

É possível copiar snapshots a partir de uma região da AWS para um Outpost. É possível fazer isso somente se os snapshots estiverem na região do Outpost. Se os snapshots estiverem em uma região diferente, é necessário copiar primeiro o snapshot para a região do Outpost e, em seguida, copiá-lo dessa região para o Outpost.

> **Note**
>
> Você não pode copiar snapshots locais de um Outpost para uma região, de um Outpost para outro ou dentro do mesmo Outpost.

É possível copiar snapshots de uma região para um Outpost usando um dos métodos a seguir.

Console

Para copiar um snapshot de uma região da AWS para um Outpost

Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

1. No painel de navegação, selecione Snapshots.
2. Selecione o snapshot e escolha Actions (Ações) e Copy (Copiar).
3. Em Destination Region (Região de destino), escolha a região para o Outpost de destino.
4. Em Snapshot Destination (Destino do snapshot), escolha AWS Outpost.

   O campo Snapshot Destination (Destino do snapshot) só será exibido se você tiver Outposts na região de destino selecionada. Se o campo não aparecer, você não terá nenhum Outpost na região de destino selecionada.

5. Em Destination Outpost ARN (ARN do Outpost de destino), insira o ARN do Outpost para o qual deseja copiar o snapshot.
6. (Opcional) Em Description (Descrição), insira uma breve descrição do snapshot copiado.
7. A criptografia é ativada por padrão para a cópia do snapshot. Não é possível desativar a criptografia. Para Chave do KMS, escolha o Chave do KMS a ser usado.
8. Escolha Copiar.

Command line

Para copiar um snapshot de uma região para um Outpost

Use o comando copy-snapshot (Copiar snapshot). Especifique o ID do snapshot a ser copiado, a região de onde deseja copiar o snapshot e o ARN do Outpost de destino.

Por exemplo, o comando a seguir copia o snapshot `snap-1234567890abcdef0` da região `us-east-1` para o Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 copy-snapshot --source-region us-east-1 --source-snapshot-
id snap-1234567890abcdef0 --destination-outpost-arn arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0 --description "Local snapshot copy"
```

Copiar AMIs de uma região da AWS para um Outpost

É possível copiar AMIs de uma região da AWS para um Outpost. Quando você copia uma AMI de uma região para um Outpost, todos os snapshots associados à AMI são copiados da região para o Outpost.

É possível copiar uma AMI de uma região para uma Outpost somente se os snapshots associados à AMI estiverem na região do Outpost. Se os snapshots estiverem em uma região diferente, é necessário copiar primeiro a AMI para a região do Outpost e, em seguida, copiá-lo dessa região para o Outpost.

> **Note**
>
> Você não pode copiar uma AMI de um Outpost para uma região, de um Outpost para outro ou dentro de um Outpost.

É possível copiar AMIs de uma região para um Outpost usando somente a AWS CLI.

Command line

Para copiar uma AMI de uma região para um Outpost

Use o comando copy-image (Copiar imagem). Especifique o ID da AMI a ser copiada, a região de origem e o ARN do Outpost de destino.

Por exemplo, o comando a seguir copia a AMI `ami-1234567890abcdef0` da região `us-east-1` para o Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 copy-image --source-region us-east-1 --source-image-
id ami-1234567890abcdef0 --name "Local AMI copy"  --destination-outpost-arn
 arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0
```

Crie volumes a partir de snapshots locais

É possível criar volumes em Outposts a partir de snapshots locais. Os volumes devem ser criados no mesmo Outpost que os snapshots de origem. Você não pode usar snapshots locais para criar volumes na região para o Outpost.

Ao criar um volume a partir de um snapshot local, você não pode criptografar novamente o volume usando uma Chave do KMS de criptografia diferente. Os volumes criados de snapshots locais devem ser criptografados usando a mesma Chave do KMS que o snapshot de origem.

Para obter mais informações, consulte Criar um volume a partir de um snapshot.

Execute instâncias a partir de AMIs baseadas em snapshots locais

É possível executar instâncias de AMIs baseadas em snapshots locais. Execute instâncias no mesmo Outpost que a AMI de origem. Para obter mais informações, consulte Launch an instance on your Outpost (Executar uma instância no Outpost) no Guia do usuário do AWS Outposts.

Exclua snapshots locais

É possível excluir snapshots locais de um Outpost. Depois de excluir um snapshot de um Outpost, a capacidade de armazenamento do Amazon S3 usada pelo snapshot excluído fica disponível por 72 horas após a exclusão do snapshot e de volumes que fazem referência a esse snapshot.

Como a capacidade de armazenamento do Amazon S3 não fica disponível de forma imediata, recomendamos que você use alarmes Amazon CloudWatch para monitorar a sua capacidade de armazenamento do Amazon S3. Exclua snapshots e volumes de que não precisa mais; assim você previne o fim da capacidade de armazenamento.

Para obter mais informações sobre como excluir snapshots, consulte Excluir um snapshot.

Automatize snapshots em um Outpost

É possível criar políticas de ciclo de vida do snapshot do Amazon Data Lifecycle Manager que criam, copiam, retêm e excluem snapshots de forma automática de seus volumes e instâncias em um Outpost. É possível escolher se deseja armazenar os snapshots em uma região ou armazená-los localmente em um Outpost. Além disso, é possível copiar automaticamente snapshots criados e armazenados em uma região da AWS para um Outpost.

A tabela a seguir oferece uma visão geral dos atributos compatíveis.

Localização do recurso	Destino do snapshot	Cópia entre regiões		Restauração rápida de snapshots	Compartilhamento entre contas
		Para a região	Para o Outpost		
Region	Region	✓	✓	✓	✓
Outpost	Region	✓	✓	✓	✓
Outpost	Outpost	✗	✗	✗	✗

Considerações

- No momento, há suporte apenas para as políticas de ciclo de vida de snapshots do Amazon EBS. Não há suporte para políticas de AMI baseadas no EBS e políticas de eventos de compartilhamento entre contas.
- Se uma política gerencia snapshots para volumes ou instâncias em uma região, os snapshots são criados na mesma região que o recurso de origem.
- Se uma política gerencia snapshots para volumes ou instâncias em um Outpost, os snapshots poderão ser criados no Outpost de origem ou na região desse Outpost.

- Uma única política não pode gerenciar snapshots em uma região e snapshots em um Outpost. Se precisar automatizar snapshots em uma região e em um Outpost, crie políticas separadas.
- Não há suporte para a restauração rápida de snapshots para snapshots criados em um Outpost ou copiados para um Outpost.
- Não há suporte para o compartilhamento entre contas para snapshots criados em um Outpost.

Para obter mais informações sobre a criação de um ciclo de vida de snapshot que gerencia snapshots locais, consulte Automating snapshot lifecycles (Como automatizar ciclos de vida de snapshots).

Criptografia do Amazon EBS

Use Criptografia de Amazon EBS como solução de criptografia direta para seus recursos do EBS associados às instâncias do EC2. Com a criptografia do Amazon EBS, não é necessário criar, manter e proteger sua própria infraestrutura de gerenciamento de chaves. A criptografia do Amazon EBS usa AWS KMS keys ao criar volumes e snapshots criptografados.

As operações de criptografia ocorrem nos servidores que hospedam instâncias do EC2, garantindo a segurança de uma instância data-at-rest e data-in-transit entre ela e seu armazenamento EBS conectado.

É possível anexar volumes criptografados e não criptografados a uma instância simultaneamente.

Tópicos

Como funciona a criptografia do EBS

É possível criptografar os volumes de dados e inicialização de uma instância do EC2.

Quando você cria um volume do EBS criptografado e o anexa a um tipo de instância com suporte, os seguintes tipos de dados são criptografados:

- Dados em repouso dentro do volume
- Todos os dados que são movidos entre o volume e a instância
- Todos os snapshots criados a partir do volume
- Todos os volumes criados a partir desses snapshots

O Amazon EBS criptografa o volume com uma chave de dados usando a criptografia de dados AES-256 padrão do setor. A chave de dados é gerada AWS KMS e depois criptografada AWS

KMS com sua AWS KMS chave antes de ser armazenada com as informações do volume. Todos os instantâneos e todos os volumes subsequentes criados a partir desses instantâneos usando a mesma AWS KMS chave compartilham a mesma chave de dados. Para obter mais informações, consulte Chaves de dados no Guia do desenvolvedor do AWS Key Management Service).

O Amazon EC2 trabalha com o Amazon EC2 AWS KMS para criptografar e descriptografar seus volumes do EBS de maneiras ligeiramente diferentes, dependendo se o snapshot a partir do qual você cria um volume criptografado é criptografado ou não criptografado.

Como funciona a criptografia EBS quando o snapshot é criptografado

Quando você cria um volume criptografado a partir de um snapshot criptografado de sua propriedade, o Amazon EC2 trabalha AWS KMS com ele para criptografar e descriptografar seus volumes do EBS da seguinte forma:

1. O Amazon EC2 envia uma GenerateDataKeyWithoutPlaintextsolicitação para AWS KMS, especificando a chave KMS que você escolheu para criptografia de volume.
2. Se o volume for criptografado usando a mesma chave KMS do instantâneo, AWS KMS usa a mesma chave de dados do instantâneo e o criptografa com a mesma chave KMS. Se o volume for criptografado usando uma chave KMS diferente, AWS KMS gera uma nova chave de dados e a criptografa com a chave KMS que você especificou. A chave de dados criptografada é enviada para ser armazenada no Amazon EBS com os metadados do volume.
3. Quando você anexa o volume criptografado a uma instância, o Amazon EC2 envia uma CreateGrantsolicitação para que AWS KMS possa descriptografar a chave de dados.
4. AWS KMS descriptografa a chave de dados criptografada e envia a chave de dados descriptografada para o Amazon EC2.
5. O Amazon EC2 usa a chave de dados de texto simples no hardware do Nitro para criptografar a E/S de disco para o volume. A chave de dados de texto simples persistirá na memória enquanto o volume estiver anexado à instância.

Como funciona a criptografia EBS quando o snapshot não é criptografado

Quando você cria um volume criptografado em um snapshot não criptografado, o Amazon EC2 trabalha com o AWS KMS para criptografar e descriptografar os volumes do EBS da seguinte forma:

1. O Amazon EC2 envia uma CreateGrantsolicitação para AWS KMS, para que possa criptografar o volume criado a partir do snapshot.

2. O Amazon EC2 envia uma GenerateDataKeyWithoutPlaintextsolicitação para AWS KMS, especificando a chave KMS que você escolheu para criptografia de volume.
3. AWS KMS gera uma nova chave de dados, a criptografa sob a chave KMS que você escolheu para criptografia de volume e envia a chave de dados criptografada para o Amazon EBS para ser armazenada com os metadados do volume.
4. O Amazon EC2 envia uma solicitação Decrypt para descriptografar AWS KMS a chave de dados criptografada, que depois é usada para criptografar os dados do volume.
5. Quando você anexa o volume criptografado a uma instância, o Amazon EC2 envia uma CreateGrantsolicitação para AWS KMS que possa descriptografar a chave de dados.
6. Quando você anexa o volume criptografado a uma instância, o Amazon EC2 envia uma solicitação Decrypt para AWS KMS, especificando a chave de dados criptografada.
7. AWS KMS descriptografa a chave de dados criptografada e envia a chave de dados descriptografada para o Amazon EC2.
8. O Amazon EC2 usa a chave de dados de texto simples no hardware do Nitro para criptografar a E/S de disco para o volume. A chave de dados de texto simples persistirá na memória enquanto o volume estiver anexado à instância.

Para obter mais informações, consulte Como o Amazon Elastic Block Store (Amazon EBS) usa o AWS KMS e exemplo dois do Amazon EC2 no Guia do desenvolvedor do AWS Key Management Service .

Como as chaves do KMS inutilizáveis afetam as chaves de dados

Quando uma chave do KMS torna-se inutilizável, o efeito é quase imediato (sujeito a consistência posterior). O estado de chave da chave do KMS é alterado para refletir sua nova condição, e todas as solicitações para usar a chave do KMS em operações de criptografia falham.

Ao executar uma ação que inutiliza a chave do KMS, não há nenhum efeito imediato sobre a instância do EC2 nem sobre os volumes do EBS anexados. O Amazon EC2 usa a chave de dados (e não a chave do KMS) para criptografar toda a E/S de disco enquanto o volume está anexado à instância.

No entanto, quando o volume criptografado do EBS é desanexado da instância do EC2, o Amazon EBS remove a chave de dados do hardware do Nitro. Da próxima vez que o volume do EBS for anexado à instância do EC2, a anexação falhará porque o Amazon EBS não consegue usar a chave

do KMS para descriptografar a chave de dados criptografada do volume. Para usar o volume do EBS novamente, é necessário tornar a chave do KMS utilizável novamente.

> **Tip**
>
> Se você não quiser mais acessar os dados armazenados em um volume do EBS criptografado com uma chave de dados gerada de uma chave do KMS que pretende tornar inutilizável, recomendamos desanexar o volume do EBS da instância do EC2 antes de tornar a chave do KMS inutilizável.

Para obter mais informações, consulte How unusable KMS keys affect data keys no Guia do desenvolvedor do AWS Key Management Service .

Requisitos da criptografia do Amazon EBS

Antes de começar, verifique se os seguintes requisitos foram atendidos.

Requisitos

- Tipos de volume compatíveis
- Tipos de instâncias compatíveis
- Permissões para usuário
- Permissões para instâncias

Tipos de volume compatíveis

A criptografia é compatível com todos os tipos de volume do EBS. É possível esperar a mesma performance de IOPS dos volumes não criptografados nos volumes criptografados, com efeito mínimo na latência. É possível acessar volumes criptografados da mesma forma que acessa volumes não criptografados. A criptografia e a descriptografia são tratadas de forma transparente e não requerem nenhuma ação adicional de sua parte e de suas aplicações.

Tipos de instâncias compatíveis

A criptografia do Amazon EBS está disponível em todos os tipos de instância da geração atual e da geração anterior.

Permissões para usuário

Quando você usa uma chave KMS para criptografia do EBS, a política de chaves do KMS permite que qualquer usuário com acesso às AWS KMS ações necessárias use essa chave do KMS para criptografar ou descriptografar recursos do EBS. É necessário conceder aos usuários do IAM a permissão para chamar as seguintes ações para usar a criptografia do EBS:

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:ReEncrypt`

> **Tip**
>
> Para seguir o princípio de menor privilégio, não permita acesso total a `kms:CreateGrant`. Em vez disso, use a chave de `kms:GrantIsForAWSResource` condição para permitir que o usuário crie concessões na chave KMS somente quando a concessão for criada em nome do usuário por um AWS serviço, conforme mostrado no exemplo a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-
a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
```

```
}
```

Para obter mais informações, consulte Permite acesso à AWS conta e ativa políticas do IAM na seção Política de chaves padrão no Guia do AWS Key Management Service desenvolvedor.

Permissões para instâncias

Quando uma instância tenta interagir com uma AMI, volume ou snapshot criptografado, uma concessão de chave do KMS é emitida para o perfil somente de identidade da instância. O perfil somente de identidade é um perfil do IAM usado pela instância para interagir com AMIs, volumes ou snapshots criptografados em seu nome.

Os perfis somente de identidade não precisam ser criados ou excluídos manualmente e não possuem políticas associadas a eles. Além disso, não é possível acessar as credenciais do perfil somente de identidade.

> **Note**
>
> As funções somente de identidade não são usadas pelos aplicativos em sua instância para acessar outros recursos AWS KMS criptografados, como objetos do Amazon S3 ou tabelas do Dynamo DB. Essas operações são feitas usando as credenciais de uma função de instância do Amazon EC2 ou AWS outras credenciais que você configurou na sua instância.

As funções somente de identidade estão sujeitas a políticas de controle de serviços (SCPs) e políticas de chaves do KMS. Se uma chave do SCP ou KMS negar ao perfil somente de identidade o acesso a uma chave do KMS, talvez você não consiga iniciar instâncias do EC2 com volumes criptografados ou usar AMIs ou instantâneos criptografados.

Se você estiver criando um SCP ou uma política de chaves que negue o acesso com base na localização da rede usando as chaves de condição `aws:SourceIp` `aws:VpcSourceIpaws:SourceVpc`,, ou `aws:SourceVpce` AWS globais, certifique-se de que essas declarações de política não se apliquem às funções somente de instância. Para obter exemplos de políticas, consulte Exemplos de políticas de perímetros de dados.

Os ARNs dos perfis somente de identidade usam o seguinte formato:

```
arn:aws-partition:iam::account_id:role/aws:ec2-infrastructure/instance_id
```

Quando uma concessão de chave é emitida para uma instância, a concessão de chave é emitida para a sessão do perfil assumido específica dessa instância. O ARN principal do beneficiário usa o seguinte formato:

```
arn:aws-partition:sts::account_id:assumed-role/aws:ec2-infrastructure/instance_id
```

Como trabalhar com a criptografia do Amazon EBS

Use os procedimentos a seguir para trabalhar com a criptografia do Amazon EBS.

Tarefas

- Selecionar uma chave do KMS para criptografia do EBS
- Habilitar a criptografia por padrão
- Gerenciar a criptografia por padrão usando a API e a CLI

Selecionar uma chave do KMS para criptografia do EBS

O Amazon EBS cria automaticamente um exclusivo Chave gerenciada pela AWS em cada região em que você armazena AWS recursos. Essa Chave do KMS tem o alias `alias/aws/ebs`. Por padrão, o Amazon EBS usa essa Chave do KMS para a criptografia. Como alternativa, é possível especificar uma chave de criptografia simétrica gerenciada pelo cliente criada como chave padrão do KMS para a criptografia EBS. Usar sua própria Chave do KMS oferece a você mais flexibilidade, incluindo a capacidade de criar, alternar e desabilitar Chaves do KMS.

> **Important**
>
> O Amazon EBS não é compatível com chaves do KMS assimétricas. Para obter mais informações, consulte Uso de chaves do KMS de criptografia simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service .

Amazon EC2 console

Como configurar a Chave do KMS padrão para a criptografia do EBS em uma região

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região.

3. No painel de navegação, selecione EC2 Dashboard (Painel do EC2).
4. No canto superior direito da página, escolha Atributos da conta, Proteção de dados e segurança.
5. Escolha Gerenciar.
6. Para a Chave de criptografia padrão, escolha uma chave de criptografia simétrica gerenciada pelo cliente.
7. Escolha Update EBS encryption (Atualizar criptografia do EBS).

Habilitar a criptografia por padrão

Você pode configurar sua AWS conta para aplicar a criptografia dos novos volumes do EBS e das cópias de snapshot que você criar. Por exemplo, o Amazon EBS criptografará os volumes do EBS criados quando você executar uma instância e os snapshots que copiar a partir de um snapshot não criptografado. Para obter exemplos da transição de recursos do EBS não criptografados para criptografados, consulte Criptografar recursos não criptografados.

Por padrão, a criptografia não tem efeito sobre volumes ou snapshots do EBS existentes.

Considerações

- A criptografia por padrão é uma configuração específica da região. Se você habilitá-la para uma região, não será possível desabilitá-la para snapshots ou volumes individuais nessa região.
- A criptografia do Amazon EBS é compatível, por padrão, com todos os tipos de instância da geração atual e da geração anterior.
- Se você copiar um snapshot e criptografá-lo com uma nova chave do KMS, será criada uma cópia completa (não incremental). Isso resulta em custos adicionais de armazenamento.
- Ao migrar servidores usando AWS Server Migration Service (SMS), não ative a criptografia por padrão. Se a criptografia por padrão já estiver ativada, e você estiver enfrentando falhas de replicação delta, desative a criptografia por padrão. Em vez disso, habilite a criptografia de AMI ao criar o trabalho de replicação.

Amazon EC2 console

Para ativar a criptografia por padrão para uma região

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. Na barra de navegação, selecione a região.
3. No painel de navegação, selecione EC2 Dashboard (Painel do EC2).
4. No canto superior direito da página, escolha Atributos da conta, Proteção de dados e segurança.
5. Escolha Gerenciar.
6. Selecione Enable (Habilitar). Você mantém o Chave gerenciada pela AWS com o alias `alias/aws/ebs` criado em seu nome como a chave de criptografia padrão ou escolhe uma chave de criptografia simétrica gerenciada pelo cliente.
7. Escolha Update EBS encryption (Atualizar criptografia do EBS).

AWS CLI

Para visualizar a criptografia por configuração padrão

- Para uma região específica

```
$ aws ec2 get-ebs-encryption-by-default --region region
```

- Para todas as regiões em sua conta

```
$ for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text); do   default=$(aws ec2 get-ebs-encryption-by-default
 --region $region --query "{Encryption_By_Default:EbsEncryptionByDefault}" --
output text); kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId'); echo "$region  --- $default  --- $kms_key"; done
```

Para habilitar a criptografia por padrão

- Para uma região específica

```
$ aws ec2 enable-ebs-encryption-by-default --region region
```

- Para todas as regiões em sua conta

```
$ for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text); do   default=$(aws ec2 enable-ebs-encryption-by-
default --region $region --query "{Encryption_By_Default:EbsEncryptionByDefault}"
```

```
 --output text); kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region |
 jq '.KmsKeyId'); echo "$region  --- $default  --- $kms_key"; done
```

Para desabilitar a criptografia por padrão

- Para uma região específica

```
$ aws ec2 disable-ebs-encryption-by-default --region region
```

- Para todas as regiões em sua conta

```
$ for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text); do   default=$(aws ec2 disable-ebs-encryption-by-
default --region $region --query "{Encryption_By_Default:EbsEncryptionByDefault}"
 --output text); kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region |
 jq '.KmsKeyId'); echo "$region  --- $default  --- $kms_key"; done
```

PowerShell

Para visualizar a criptografia por configuração padrão

- Para uma região específica

```
PS C:\> Get-EC2EbsEncryptionByDefault -Region region
```

- Para todas as regiões em sua conta

```
PS C:\> (Get-EC2Region).RegionName | ForEach-Object { [PSCustomObject]@{ Region
 = $_; EC2EbsEncryptionByDefault = Get-EC2EbsEncryptionByDefault -Region $_;
 EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_ } } | Format-Table -
AutoSize
```

Para habilitar a criptografia por padrão

- Para uma região específica

```
PS C:\> Enable-EC2EbsEncryptionByDefault -Region region
```

- Para todas as regiões em sua conta

```
PS C:\> (Get-EC2Region).RegionName | ForEach-Object { [PSCustomObject]@{ Region
 = $_; EC2EbsEncryptionByDefault = Enable-EC2EbsEncryptionByDefault -Region $_;
 EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_ } } | Format-Table -
AutoSize
```

Para desabilitar a criptografia por padrão

- Para uma região específica

```
PS C:\> Disable-EC2EbsEncryptionByDefault -Region region
```

- Para todas as regiões em sua conta

```
PS C:\> (Get-EC2Region).RegionName | ForEach-Object { [PSCustomObject]@{ Region
 = $_; EC2EbsEncryptionByDefault = Disable-EC2EbsEncryptionByDefault -Region $_;
 EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_ } } | Format-Table -
AutoSize
```

Não é possível alterar a Chave do KMS que está associada a um snapshot existente ou a um volume criptografado. No entanto, é possível associar uma Chave do KMS diferente durante uma operação de cópia de snapshot para que o snapshot copiado resultante seja criptografado pela nova Chave do KMS.

Gerenciar a criptografia por padrão usando a API e a CLI

É possível gerenciar a criptografia por padrão e a Chave do KMS padrão usando os comandos da CLI e ações de API a seguir.

Ação de API	Comando da CLI	Descrição
DisableEbsEncryptionByDefault	disable-ebs-encryption-by-padrão	Desativa a criptografia por padrão.
EnableEbsEncryptionByDefault	enable-ebs-encryption-by-padrão	Ativa a criptografia por padrão.

Ação de API	Comando da CLI	Descrição
GetEbsDefaultKmsKeyId	get-ebs-default-kms-ID da chave	Descreve a Chave do KMS padrão.
GetEbsEncryptionByDefault	get-ebs-encryption-by-padrão	Indica se a criptogra fia por padrão está ativada.
ModifyEbsDefaultKmsKeyId	modify-ebs-default-kms-ID da chave	Altera a Chave do KMS padrão usada para criptografar volumes do EBS.
ResetEbsDefaultKmsKeyId	reset-ebs-default-kms-ID da chave	Redefine a Chave gerenciada pela AWS como chave KMS padrão usada para criptografar volumes do EBS.

Criptografar recursos do EBS

Criptografe volumes do EBS habilitando a criptografia, usando a criptografia por padrão ou habilitando a criptografia ao criar um volume que deseja criptografar.

Ao criptografar um volume, é possível especificar a chave do KMS de criptografia simétrica a ser usada para criptografar o volume. Se a Chave do KMS não for especificada, a Chave do KMS usada para a criptografia dependerá do estado de criptografia do snapshot de origem e de sua propriedade. Para obter mais informações, consulte a tabela de resultados de criptografia.

> **Note**
>
> Se você estiver usando a API ou AWS CLI para especificar uma chave KMS, saiba que ela AWS autentica a chave KMS de forma assíncrona. Se você especificar um ID de Chave do KMS, um alias ou um ARN que não forem válidos, é possível que a ação pareça estar concluída, mas ela falhará eventualmente.

Você não pode alterar a Chave do KMS que estiver associada a um snapshot ou a um volume existente. No entanto, é possível associar uma Chave do KMS diferente durante uma operação de cópia de snapshot para que o snapshot copiado resultante seja criptografado pela nova Chave do KMS.

Criptografar um volume vazio na criação

Ao criar um novo volume do EBS vazio, será possível criptografá-lo habilitando a criptografia para a operação de criação de volume específica. Se você tiver habilitado a criptografia do EBS por padrão, o volume será automaticamente criptografado usando a Chave do KMS padrão para criptografia do EBS. Outra opção é especificar uma chave do KMS de criptografia simétrica diferente para a operação de criação de um volume específico. O volume será criptografado no momento em que for disponibilizado a primeira vez, para que seus dados estejam sempre protegidos. Para ver os procedimentos detalhados, consulte Crie um volume do Amazon EBS..

Por padrão, a Chave do KMS selecionada durante a criação de um volume criptografa os snapshots que você cria do volume e os volumes que você restaura desses snapshots criptografados. Não é possível remover a criptografia de um volume ou snapshot criptografado, o que significa que um volume restaurado a partir de um snapshot criptografado ou uma cópia de um snapshot criptografado será sempre criptografado.

Não há suporte para snapshots públicos de volumes criptografado, mas é possível compartilhar um snapshot criptografado com contas específicas. Para obter instruções detalhadas, consulte Compartilhar um snapshot do Amazon EBS.

Criptografar recursos não criptografados

Não é possível criptografar diretamente volumes ou snapshots não criptografados. No entanto, é possível criar volumes ou snapshots criptografados a partir de volumes ou snapshots não criptografados. Se você habilitar a criptografia por padrão, o Amazon EBS automaticamente criptografa o novo volume ou snapshot usando a chave KMS padrão para a criptografia do EBS. Caso contrário, será possível habilitar a criptografia ao criar um volume ou um snapshot individual, usando a Chave KMS padrão para a criptografia do Amazon EBS ou uma chave de criptografia simétrica gerenciada pelo cliente. Para obter mais informações, consulte Crie um volume do Amazon EBS. e Copiar um snapshot do Amazon EBS..

Para criptografar a cópia do snapshot para uma chave gerenciada pelo cliente, é necessário habilitar a criptografia e especificar a Chave do KMS, conforme mostrado em Copiar um snapshot não criptografado (criptografia por padrão não habilitada).

> **Important**
>
> O Amazon EBS não é compatível com chaves do KMS assimétricas. Para obter mais informações, consulte Uso de chaves do KMS de criptografia simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service .

Também é possível aplicar novos estados de criptografia ao executar uma instância a partir de uma AMI baseada em EBS. Isso ocorre porque as AMIs baseadas em EBS incluem snapshots de volumes do EBS que podem ser criptografados conforme descrito. Para obter mais informações, consulte Usar criptografia com AMIs baseadas no EBS.

Teclas rotativas AWS KMS

As melhores práticas criptográficas desencorajam a reutilização extensiva de chaves de criptografia.

Para criar um novo material criptográfico para uso com a criptografia do Amazon EBS, você pode criar uma nova chave gerenciada pelo cliente e, em seguida, alterar seus aplicativos para usar essa nova chave KMS. Ou é possível habilitar a alternância automática de chaves para uma chave gerenciada pelo cliente existente.

Quando você ativa a rotação automática de chaves para uma chave gerenciada pelo cliente, AWS KMS gera novo material criptográfico para a chave KMS todos os anos. AWS KMS salva todas as versões anteriores do material criptográfico para que você possa continuar a descriptografar e usar volumes e instantâneos previamente criptografados com esse material de chave KMS. AWS KMS não exclui nenhum material de chave girada até que você exclua a chave KMS.

Quando você usa uma chave rotativa gerenciada pelo cliente para criptografar um novo volume ou snapshot, AWS KMS usa o material de chave atual (novo). Quando você usa uma chave rotativa gerenciada pelo cliente para descriptografar um volume ou instantâneo, AWS KMS usa a versão do material criptográfico que foi usado para criptografá-lo. Se um volume ou instantâneo for criptografado com uma versão anterior do material criptográfico, AWS KMS continue usando essa versão anterior para descriptografá-lo. AWS KMS não criptografa novamente volumes ou instantâneos previamente criptografados para usar o novo material criptográfico após uma rotação de chave. Eles permanecem criptografados com o material criptográfico com o qual foram originalmente criptografados. Você pode usar com segurança uma chave rotativa gerenciada pelo cliente em aplicativos e AWS serviços sem alterações no código.

> **Note**
>
> - A rotação automática de chaves é suportada somente para chaves simétricas gerenciadas pelo cliente com material de chave que AWS KMS cria.
> - AWS KMS gira automaticamente a Chaves gerenciadas pela AWS cada ano. Não é possível habilitar ou desabilitar a alternância de chaves para Chaves gerenciadas pela AWS.

Para obter mais informações, consulte Rotating KMS key (Alternar chave do KMS) no Guia do desenvolvedor do AWS Key Management Service .

Exemplos de criptografia do Amazon EBS

Quando você cria um recurso do EBS criptografado, ele é criptografado pela Chave do KMS padrão para a criptografia do EBS da sua conta, a menos que você especifique uma chave gerenciada pelo cliente diferente nos parâmetros de criação do volume ou no mapeamento de dispositivos de blocos para a AMI ou para a instância. Para ter mais informações, consulte Selecionar uma chave do KMS para criptografia do EBS.

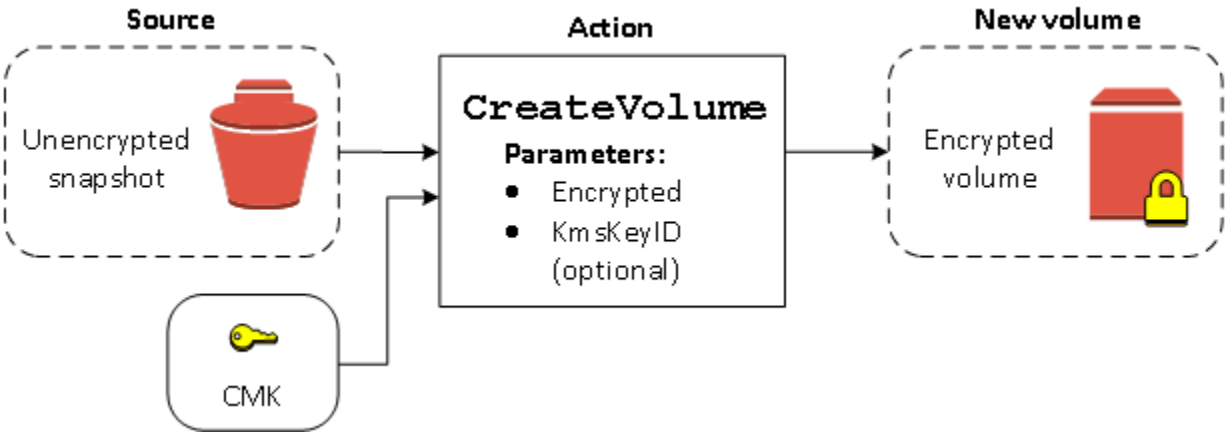
Os exemplos a seguir ilustram como é possível gerenciar o estado de criptografia de seus volumes e snapshots. Para obter uma lista completa de casos de criptografia, consulte a tabela de resultados de criptografia.

Exemplos

- Restaurar um volume não criptografado (criptografia por padrão não habilitada)
- Restaurar um volume não criptografado (criptografia por padrão habilitada)
- Copiar um snapshot não criptografado (criptografia por padrão não habilitada)
- Copiar um snapshot não criptografado (criptografia por padrão habilitada)
- Criptografar novamente um volume criptografado
- Criptografar novamente um snapshot criptografado
- Migrar dados entre volumes criptografados e não criptografados
- Resultados da criptografia

Restaurar um volume não criptografado (criptografia por padrão não habilitada)

Sem a criptografia por padrão habilitada, um volume restaurado de um snapshot não criptografado é não criptografado por padrão. No entanto, é possível criptografar o volume resultante configurando o parâmetro `Encrypted` e, opcionalmente, o parâmetro `KmsKeyId`. O diagrama a seguir ilustra o processo.

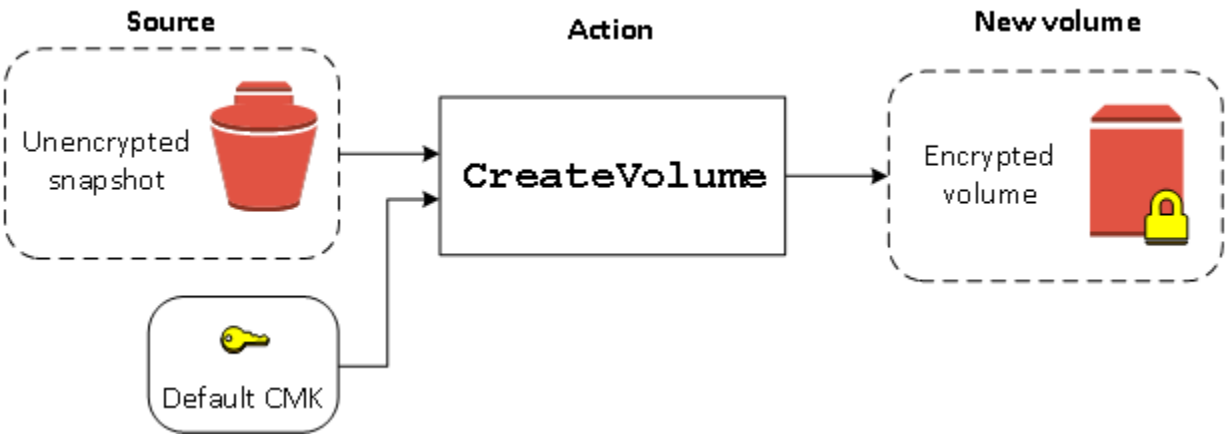


Se você deixar o parâmetro `KmsKeyId` de fora, o volume resultante será criptografado usando a Chave do KMS padrão para a criptografia do EBS. Especifique o ID de uma Chave do KMS para criptografar o volume de uma Chave do KMS diferente.

Para obter mais informações, consulte Criar um volume a partir de um snapshot.

Restaurar um volume não criptografado (criptografia por padrão habilitada)

Quando a criptografia for habilitada por padrão, ela será obrigatória para volumes restaurados de snapshots não criptografados, e nenhum parâmetro de criptografia será necessário para que a Chave do KMS padrão seja usada. O diagrama a seguir mostra este simples caso padrão:

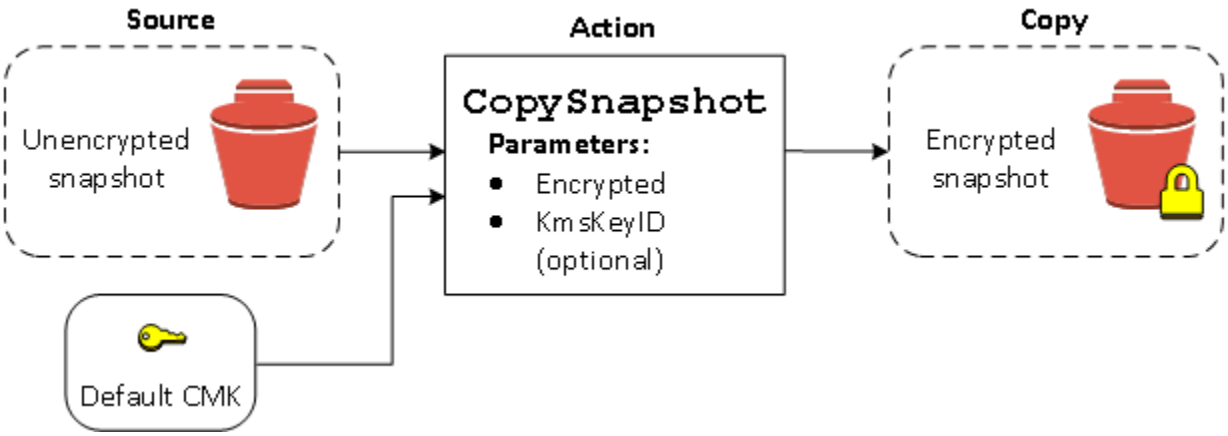


Se quiser criptografar o volume restaurado com uma chave de criptografia simétrica gerenciada pelo cliente, você deverá fornecer os parâmetros `Encrypted` e `KmsKeyId`, conforme mostrado em Restaurar um volume não criptografado (criptografia por padrão não habilitada).

Copiar um snapshot não criptografado (criptografia por padrão não habilitada)

Sem a criptografia por padrão habilitada, uma cópia de um snapshot não criptografado é não criptografado por padrão. No entanto, é possível criptografar o snapshot resultante configurando o parâmetro `Encrypted` e, opcionalmente, o parâmetro `KmsKeyId`. Se você omitir o `KmsKeyId`, o snapshot resultante será criptografado pela Chave do KMS padrão. É necessário especificar o ID de uma chave do KMS de criptografia para criptografar o volume para uma chave do KMS de criptografia simétrica diferente.

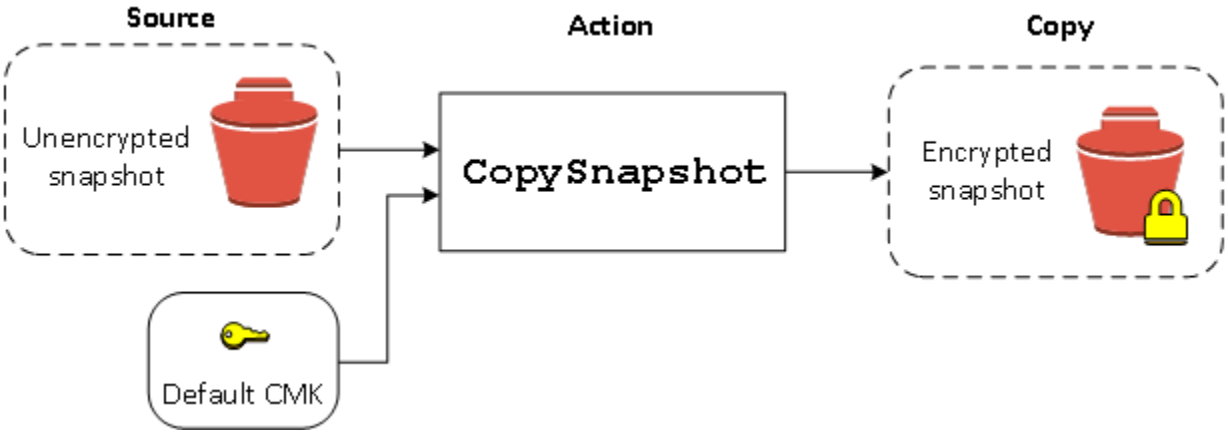
O diagrama a seguir ilustra o processo.



É possível criptografar um volume do EBS ao copiar um snapshot não criptografado em um snapshot criptografado e criar um volume a partir do snapshot criptografado. Para obter mais informações, consulte Copiar um snapshot do Amazon EBS..

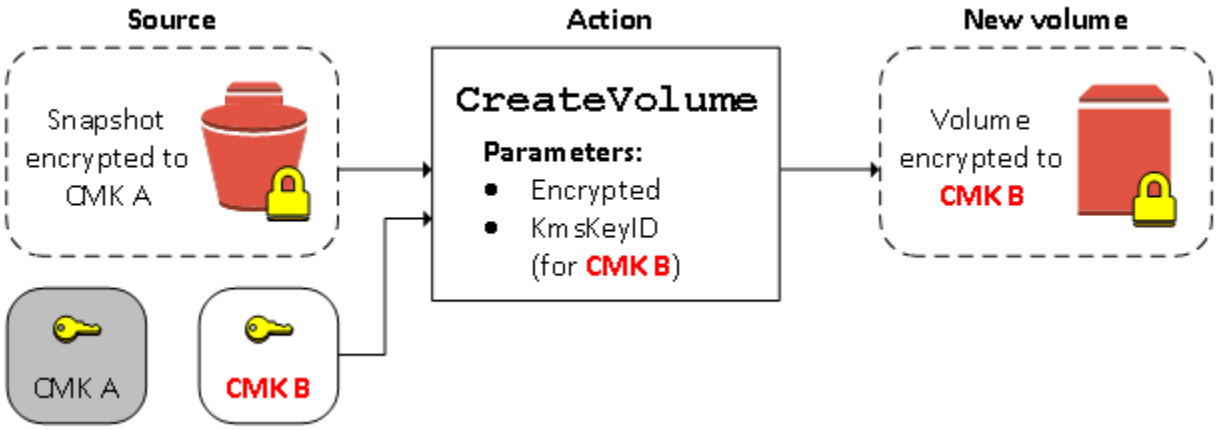
Copiar um snapshot não criptografado (criptografia por padrão habilitada)

Quando a criptografia por padrão estiver habilitada, a criptografia é obrigatória para cópias de snapshots não criptografados, e nenhum parâmetro de criptografia será necessário se a Chave do KMS padrão for usada. O diagrama a seguir ilustra este caso padrão:



Criptografar novamente um volume criptografado

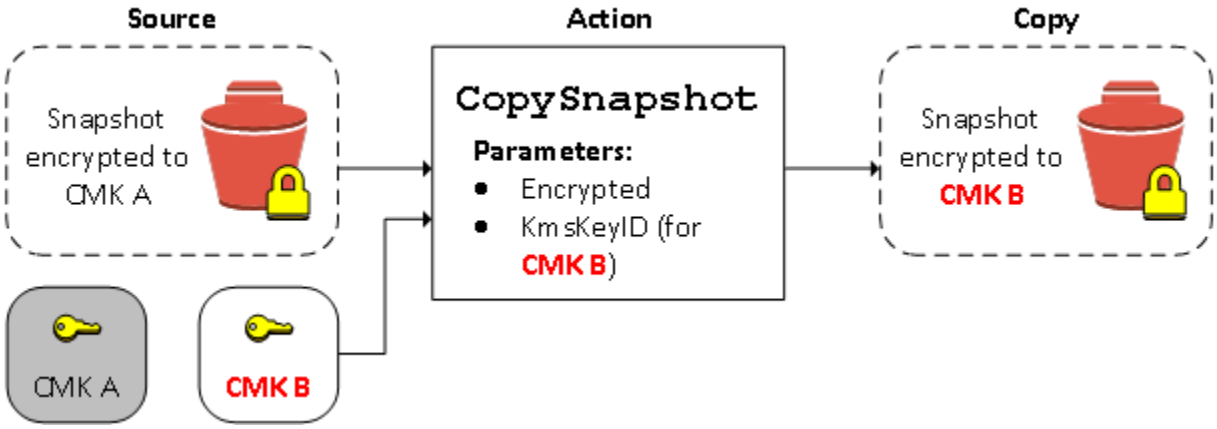
Quando a ação `CreateVolume` opera em um snapshot criptografado, você tem a opção de criptografá-lo novamente com uma Chave do KMS diferente. O diagrama a seguir ilustra o processo. Neste exemplo, você tem duas Chaves do KMS: Chave do KMS A e Chave do KMS B. O snapshot de origem é criptografado pela Chave do KMS A. Durante a criação do volume, com o ID de Chave do KMS da Chave do KMS B especificado como um parâmetro, os dados de origem são automaticamente descriptografados e, depois, novamente criptografados pela Chave do KMS B.



Para obter mais informações, consulte Criar um volume a partir de um snapshot.

Criptografar novamente um snapshot criptografado

A capacidade de criptografar um snapshot durante a cópia permite aplicar uma nova Chave do KMS de criptografia simétrica a um snapshot já criptografado de sua propriedade. Os volumes restaurados da cópia resultante só são acessíveis usando a nova Chave do KMS. O diagrama a seguir ilustra o processo. Neste exemplo, você tem duas Chaves do KMS: Chave do KMS A e Chave do KMS B. O snapshot de origem é criptografado pela Chave do KMS A. Durante a cópia, com o ID de Chave do KMS da Chave do KMS B especificado como um parâmetro, os dados de origem são novamente criptografados de forma automática pela Chave do KMS B.



Em um cenário relacionado, é possível optar por aplicar novos parâmetros de criptografia a uma cópia de um snapshot que tenha sido compartilhado com você. Por padrão, a cópia é criptografada com uma Chave do KMS compartilhada pelo proprietário do snapshot. No entanto, recomendamos que você crie uma cópia do snapshot compartilhado usando uma Chave do KMS diferente que esteja sob seu controle. Isso protegerá seu acesso ao volume se a Chave do KMS original estiver comprometida ou se o proprietário revogar a Chave do KMS por algum motivo. Para obter mais informações, consulte Cópia de snapshot e criptografia.

Migrar dados entre volumes criptografados e não criptografados

Quando você tem acesso a volumes criptografados e não criptografados, pode transferir livremente dados entre eles. O EC2 realiza as operações de criptografia ou descriptografia de forma transparente.

Instâncias do Linux

Por exemplo: use o comando rsync para copiar os dados. No comando a seguir, os dados de origem estão localizados em `/mnt/source` e o volume de destino está montado em `/mnt/destination`.

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

Instâncias do Windows

Por exemplo: use o comando robocopy para copiar os dados. No comando a seguir, os dados de origem estão localizados em `D:\` e o volume de destino está montado em `E:\`.

```
PS C:\> robocopy D:\sourcefolder E:\destinationfolder /e /copyall /eta
```

É recomendável usar pastas, em vez de copiar um volume inteiro, para evitar possíveis problemas com pastas ocultas.

Resultados da criptografia

A tabela a seguir descreve o resultado da criptografia para cada combinação possível de configurações.

A criptografia está ativada?	A criptografia está ativada por padrão?	Origem do volume	Padrão (nenhuma chave gerenciada pelo cliente especificada)	Personalizado (chave gerenciada pelo cliente especificada)
Não	Não	Novo volume (vazio)	Não criptografado	N/D
Não	Não	Snapshot não criptografado pertencente a você	Não criptografado	
Não	Não	Snapshot criptografado pertencente a você	Criptografado pela mesma chave	
Não	Não	Snapshot não criptografado compartilhado com você	Não criptografado	

A criptografia está ativada?	A criptografia está ativada por padrão?	Origem do volume	Padrão (nenhuma chave gerenciada pelo cliente especificada)	Personalizado (chave gerenciada pelo cliente especificada)
Não	Não	Snapshot criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente*	
Sim	Não	Novo volume	Criptografado por chave padrão gerenciada pelo cliente	Criptografado por uma chave gerenciada pelo cliente especificada**
Sim	Não	Snapshot não criptografado pertencente a você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Não	Snapshot criptografado pertencente a você	Criptografado pela mesma chave	
Sim	Não	Snapshot não criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Não	Snapshot criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Não	Sim	Novo volume (vazio)	Criptografado por chave padrão gerenciada pelo cliente	N/D

A criptografia está ativada?	A criptografia está ativada por padrão?	Origem do volume	Padrão (nenhuma chave gerenciada pelo cliente especificada)	Personalizado (chave gerenciada pelo cliente especificada)
Não	Sim	Snapshot não criptografado pertencente a você	Criptografado por chave padrão gerenciada pelo cliente	
Não	Sim	Snapshot criptografado pertencente a você	Criptografado pela mesma chave	
Não	Sim	Snapshot não criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Não	Sim	Snapshot criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Sim	Novo volume	Criptografado por chave padrão gerenciada pelo cliente	Criptografado por uma chave gerenciada pelo cliente especificada
Sim	Sim	Snapshot não criptografado pertencente a você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Sim	Snapshot criptografado pertencente a você	Criptografado pela mesma chave	

A criptografia está ativada?	A criptografia está ativada por padrão?	Origem do volume	Padrão (nenhuma chave gerenciada pelo cliente especificada)	Personalizado (chave gerenciada pelo cliente especificada)
Sim	Sim	Snapshot não criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Sim	Snapshot criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	

* Essa é a chave padrão gerenciada pelo cliente usada para criptografia do EBS para a AWS conta e a região. Por padrão, isso é exclusivo Chave gerenciada pela AWS para o EBS, ou você pode especificar uma chave gerenciada pelo cliente. Para ter mais informações, consulte Selecionar uma chave do KMS para criptografia do EBS.

** Esta é uma chave gerenciada pelo cliente especificada para o volume no momento do lançamento. Essa chave gerenciada pelo cliente é usada em vez da chave gerenciada pelo cliente padrão para a AWS conta e a região.

Performance de volumes do Amazon EBS

Vários fatores, como as características de E/S e a configuração das instâncias e volumes, podem afetar a performance dos volumes do Amazon EBS. Ao seguir as orientações em nossas páginas de detalhes do produto do Amazon EBS e do Amazon EC2, você muito provavelmente conseguirá atingir uma boa performance. No entanto, há alguns casos em que talvez seja necessário fazer alguns ajustes para atingir a performance máxima. Recomendamos que você ajuste a performance com informações de sua workload real, além da comparação, para determinar sua configuração ideal. Após você entender os conceitos básicos de utilização dos volumes do EBS, é uma boa ideia examinar a performance de E/S necessária e as opções para melhorar a performance do Amazon EBS a fim de atender a esses requisitos.

AWS as atualizações no desempenho dos tipos de volume do EBS podem não entrar em vigor imediatamente em seus volumes existentes. Para ver a performance completa em um volume anterior, primeiro é possível precisar realizar uma ação `ModifyVolume` nele. Para ter mais informações, consulte Modificar um volume do EBS usando Volumes Elásticos do Amazon EBS.

Conteúdo

Dicas de performance do Amazon EBS

Essas dicas representam as melhores práticas para obter a performance ideal de seus volumes do EBS em uma variedade de cenários de usuário.

Usar instâncias otimizadas para EBS

Em instâncias sem suporte para a throughput otimizada para EBS, o tráfego de rede poderá competir com o tráfego entre sua instância e seus volumes do EBS. Em instâncias otimizadas para EBS, os dois tipos de tráfego são mantidos separados. Algumas configurações de instâncias otimizadas para EBS incorrem um custo extra (como C3, R3 e M3), enquanto outras são sempre otimizadas

para EBS sem custo extra (como M4, C4, C5 e D2). Para ter mais informações, consulte Otimizar a parformance do Amazon EBS.

Noções básicas de como a performance é calculada

Quando você mede a performance dos volumes do EBS, é importante compreender as unidades de medida envolvidas e como a performance é calculada. Para obter mais informações, consulte Características e monitoramento de E/S do Amazon EBS.

Noções básicas da workload

Há uma relação entre a performance máxima dos volumes do EBS, o tamanho e o número de operações de E/S e o tempo necessário para que cada ação seja concluída. Cada um desses fatores (performance, E/S e latência) afeta os outros, e aplicações diferentes são mais sensíveis em relação a um fator do que outros. Para obter mais informações, consulte Comparar volumes do EBS.

Esteja ciente da penalidade de performance ao inicializar volumes de snapshots

Há um aumento significativo da latência quando você acessa cada bloco de dados pela primeira vez em um novo volume do EBS que foi criado de um snapshot. É possível evitar essa ocorrência de performance usando uma das seguintes opções:

- Acessar cada bloco antes de colocar o volume em produção. Esse processo é chamado inicialização (conhecido anteriormente como pré-aquecimento). Para obter mais informações, consulte Inicializar volumes de Amazon EBS.
- Habilite as restauração rápida em um snapshot para garantir que os volumes do EBS criados de um snapshot sejam totalmente inicializados na criação e entreguem instantaneamente toda a sua performance provisionada. Para obter mais informações, consulte Restauração rápida de snapshots do Amazon EBS.

Fatores que podem reduzir a performance do HDD

Quando você cria um snapshot de um volume HDD otimizado para throughput (`st1`) ou HDD a frio (`sc1`), a performance poderá cair até o valor básico do volume enquanto o snapshot estiver em andamento. Esse comportamento é específico desses tipos de volumes. Outros fatores que podem limitar a performance incluem a orientação de uma throughput maior do que a instância pode oferecer suporte, a penalidade de performance encontrada ao inicializar volumes criados de um

snapshot e as quantidades excessivas de pequenas operações de E/S aleatórias no volume. Para obter mais informações sobre como calcular a throughput para volumes de HDD, consulte Tipos de volume do Amazon EBS.

A performance também pode ser afetada se sua aplicação não estiver enviando solicitações de E/S suficientes. Isso pode ser monitorado verificando o comprimento da fila do volume e o tamanho da E/S. O comprimento da fila é o número de solicitações pendentes de E/S de sua aplicação para seu volume. Para obter máxima consistência, os volumes baseados em HDD devem manter um comprimento de fila (arredondado para o número inteiro mais próximo) de 4 ou mais ao executar E/S sequencial de 1 MiB. Para obter mais informações sobre como garantir a performance consistente de seus volumes, consulte Características e monitoramento de E/S do Amazon EBS

Aumentar a leitura antecipada para workloads com muitas operações de leitura e alta throughput em `st1` e `sc1` (somente instâncias do Linux)

Algumas workloads têm muita leitura e acessam o dispositivo de blocos pelo cache da página do sistema operacional (por exemplo, de um sistema de arquivos). Nesse caso, para alcançar a throughput máxima, recomendamos que você defina a configuração de leitura antecipada como 1 MiB. Essa é uma per-block-device configuração que só deve ser aplicada aos volumes do seu HDD.

Para examinar o valor atual de leitura antecipada para os dispositivos de blocos, use o seguinte comando:

```
[ec2-user ~]$ sudo blockdev --report /dev/<device>
```

As informações do dispositivo de blocos são retornadas neste formato:

```
RO    RA   SSZ   BSZ   StartSec            Size   Device
rw   256   512  4096       4096      8587820544   /dev/<device>
```

O dispositivo mostrado relata um valor de leitura antecipada de 256 (o padrão). Multiplique esse número pelo tamanho do setor (512 bytes) para obter o tamanho de buffer de leitura antecipada, que nesse caso é 128 KiB. Para configurar o valor de buffer de 1 MiB, use o seguinte comando:

```
[ec2-user ~]$ sudo blockdev --setra 2048 /dev/<device>
```

Verifique se a configuração de leitura antecipada agora exibe 2.048 executando o primeiro comando novamente.

Use essa configuração somente quando sua workload consistir em grandes E/S sequenciais. Se consistir principalmente em pequenas E/S aleatórias, essa configuração acabará reduzindo a performance. Em geral, se sua workload consiste principalmente em operações de E/S pequenas ou aleatórias, é necessário avaliar a possibilidade de usar um volume SSD de uso geral (`gp2` e `gp3`) em vez de um volume `st1` ou `sc1`.

Use um kernel do Linux moderno (somente instâncias do Linux)

Use um kernel do Linux moderno com suporte para descritores indiretos. Qualquer kernel do Linux versão 3.8 e posterior tem esse suporte, bem como qualquer instância do EC2 da geração atual. Se o tamanho médio de E/S for igual ou próximo a 44 KiB, será possível usar uma instância ou um kernel sem suporte para descritores indiretos. Para obter informações sobre como derivar o tamanho médio de E/S das CloudWatch métricas da Amazon, consulte. Características e monitoramento de E/S do Amazon EBS

Para alcançar a throughput máxima em volumes `st1` ou `sc1`, recomendamos aplicar um valor de 256 ao parâmetro `xen_blkfront.max` (para versões de kernel do Linux abaixo de 4.6) ou o parâmetro `xen_blkfront.max_indirect_segments` (para a versão de kernel do Linux 4.6 e acima). O parâmetro apropriado pode ser definido na linha de comando de inicialização do sistema operacional.

Por exemplo, em uma AMI do Amazon Linux com um kernel mais antigo, é possível adicioná-lo ao final da linha de kernel na configuração de GRUB encontrada em `/boot/grub/menu.lst`:

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0
 xen_blkfront.max=256
```

Para um kernel mais recente, o comando será semelhante ao seguinte:

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
 xen_blkfront.max_indirect_segments=256
```

Reinicialize sua instância para que essa configuração seja implementada.

Para obter mais informações, consulte Configurar o GRUB para AMIs paravirtuais. Outras distribuições do Linux, especialmente aquelas que não usam o carregador de inicialização de GRUB, podem exigir uma abordagem diferente para ajustar os parâmetros de kernel.

Para obter mais informações sobre as características de E/S do EBS, consulte a apresentação re:Invent Amazon EBS: Como projetar visando a performance neste tópico.

Usar o RAID 0 para maximizar a utilização de recursos de instância

Alguns tipos de instância podem gerar throughput de E/S maior do que o que é possível provisionar para um único volume do EBS. É possível adicionar vários volumes juntos em uma configuração de RAID 0 para usar a largura de banda disponível para essas instâncias. Para ter mais informações, consulte Configuração do Amazon EBS e RAID.

Acompanhe o desempenho usando a Amazon CloudWatch

A Amazon Web Services fornece métricas de desempenho para o Amazon EBS que você pode analisar e visualizar com a Amazon CloudWatch e verificações de status que você pode usar para monitorar a integridade dos seus volumes. Para ter mais informações, consulte Monitorar volumes do Amazon EBS.

Otimizar a parformance do Amazon EBS

Uma instância otimizada para o Amazon EBS usa uma pilha de configuração otimizada e fornece capacidade adicional dedicada para E/S do Amazon EBS. Essa otimização proporciona a melhor performance para seus volumes do EBS ao minimizar a contenção entre a E/S do Amazon EBS e outro tráfego de sua instância.

Instâncias otimizadas para o EBS oferecem largura de banda dedicada para o Amazon EBS. Quando anexados a uma instância otimizada para EBS, os volumes de SSD de uso geral (`gp2` e `gp3`) fornecem ao menos 90% de sua performance de IOPS provisionada, 99% do tempo em um determinado ano, e os volumes de SSD com IOPS provisionadas (`io1` e `io2`) fornecem ao menos 90% de sua performance de IOPS provisionadas, 99,9% do tempo em um determinado ano. HDD otimizado para throughput (`st1`) e HDD frio (`sc1`) fornecem ao menos 90% da performance esperada de throughput, 99% do tempo em um determinado ano. Períodos não compatíveis são distribuídos com uniformidade aproximada, destinando 99% da throughput total esperada a cada hora. Para ter mais informações, consulte Tipos de volume do Amazon EBS.

Para obter mais informações, consulte Instâncias otimizadas para o Amazon EBS no Guia do usuário do Amazon EC2.

Características e monitoramento de E/S do Amazon EBS

Em uma determinada configuração de volume, certas características de E/S controlam a performance dos volumes do EBS. Volumes baseados em SSD – SSD de uso geral (`gp2` e `gp3`) e

SSD de IOPS provisionados (`io1` e `io2`) – geram performance consistente quando uma operação de E/S for aleatória ou sequencial. Volumes baseados em HDD – HDD otimizado para throughput (`st1`) e HDD a frio (`sc1`) – geram performance ideal somente quando as operações de E/S são grandes e sequenciais. Para entender como os volumes de SSD e HDD serão executados em sua aplicação, é importante saber sobre as conexões entre a demanda no volume, a quantidade de IOPS disponível para ele, o tempo necessário para que uma operação de E/S seja concluída e os limites de throughput do volume.

Tópicos

IOPS

IOPS é uma unidade de medida que representa operações de entrada/saída por segundo. As operações são medidas em KiB, e a tecnologia de disco subjacente determina a quantidade máxima de dados que um tipo de volume conta como uma única E/S. O tamanho de E/S é limitado a 256 KiB para volumes SSD e 1.024 KiB para volumes HDD porque os volumes SSD lidam com E/S pequena ou aleatória de forma muito mais eficiente do que os volumes HDD.

Quando operações de E/S pequenas são fisicamente sequenciais, o Amazon EBS tenta mesclá-las em uma única operação de E/S até o tamanho máximo de E/S. Da mesma maneira, quando operações de E/S são maiores do que o tamanho máximo de E/S, o Amazon EBS tenta dividi-las em operações de E/S menores. A tabela a seguir mostra alguns exemplos.

Tipo de volume	Tamanho máximo de E/S	Operações de E/S da sua aplicação	Número de IOPS	Observações
SSD	256 KiB	1 x operação de E/S de 1024 KiB	4 (1.024 ÷ 256 = 4)	O Amazon EBS divide a operação de E/S de 1.024 em quatro operações

Tipo de volume	Tamanho máximo de E/S	Operações de E/S da sua aplicação	Número de IOPS	Observações
				menores de 256 KiB.
		8 x operações de E/S sequenciais de 32 KiB	1 (8 x 32 = 256)	O Amazon EBS mescla as oito operações sequenciais de E/S de 32 KiB em uma única operação de 256 KiB.
		8 operações de E/S aleatórias de 32 KiB	8	O Amazon EBS conta as operações de E/S aleatórias separadamente.
HDD	1.024 KiB	1 x operação de E/S de 1024 KiB	1	A operação de E/S já é igual ao tamanho máximo de E/S. Ela não é mesclada ou dividida.
		8 x operações de E/S sequenciais de 128 KiB	1 (8 x 128 = 1.024)	O Amazon EBS mescla as oito operações sequenciais de E/S de 128 KiB em uma única operação de E/S de 1024 KiB.

Tipo de volume	Tamanho máximo de E/S	Operações de E/S da sua aplicação	Número de IOPS	Observações
		8 operações de E/S aleatórias de 32 KiB	8	O Amazon EBS conta as operações de E/S aleatórias separadamente.

Portanto, quando você cria um volume baseado em SSD com suporte a 3.000 IOPS (provisionando um volume de Provisioned IOPS SSD com 3.000 IOPS ou dimensionando um volume de Finalidade geral (SSD) com 1,000 GiB), e você o anexa a uma instância otimizada para EBS que pode fornecer largura de banda suficiente, é possível transferir até 3.000 E/S de dados por segundo, com a throughput determinada pelo tamanho de E/S.

Comprimento e latência da fila de volume

A fila de volume é o número de solicitações de E/S pendentes para um dispositivo. A latência é o tempo real do end-to-end cliente de uma operação de E/S, em outras palavras, o tempo decorrido entre o envio de uma E/S para o EBS e o recebimento de uma confirmação do EBS de que a leitura ou gravação de E/S foi concluída. O comprimento da fila deve ser adequadamente calibrado com o tamanho e a latência de E/S para evitar criar gargalos no sistema operacional convidado ou no link de rede para EBS.

O tamanho ideal da fila varia para cada workload, dependendo da sensibilidade de sua aplicação específica em relação à IOPS e à latência. Se sua workload não estiver fornecendo solicitações de E/S suficientes para usar integralmente a performance disponível para seu volume do EBS, o volume pode não fornecer a IOPS ou a throughput que você provisionou.

As aplicações com transações intensivas são sensíveis ao aumento de latência de E/S e são adequadas para volumes baseados em SSD. É possível manter a IOPS alta e, ao mesmo tempo, a latência baixa mantendo uma fila de comprimento pequeno e um alto número de IOPS disponíveis para o volume. Se você gerar consistentemente mais IOPS para um volume do que ele dispõe, poderá causar o aumento da latência de E/S.

As aplicações com throughput intensiva são menos sensíveis ao aumento da latência de E/S e são bem adequadas para volumes baseados em HDD. É possível manter alta throughput para volumes baseados em HDD mantendo uma fila de comprimento maior ao executar E/S grande e sequencial.

Limites de throughput de tamanho e volume de E/S

Para volumes baseados em SSD, se o tamanho de E/S for muito grande, será possível ter um número menor de IOPS do que provisionou, porque você está chegando ao limite de throughput do volume. Por exemplo, um volume `gp2` com menos de 1.000 GiB com créditos de expansão disponíveis tem um limite de IOPS de 3.000 e um limite de volume de throughput de 250 MiB/s. Se você estiver usando um tamanho de E/S de 256 KiB, o volume atingirá o limite da throughput a 1000 IOPS (1000 x 256 KiB = 250 MiB). Para E/S de tamanhos menores (por exemplo, 16 KiB), esse mesmo volume pode sustentar 3.000 IOPS porque a throughput está bem abaixo de 250 MiB/s. Estes exemplos supõem que a E/S do volume não atinge os limites de throughput da instância. Para obter mais informações sobre os limites de throughput para cada tipo de volume do EBS, consulte Tipos de volume do Amazon EBS.

Para operações de E/S menores, você pode ver um valor de higher-than-provisioned IOPS medido de dentro da sua instância. Isso acontece quando o sistema operacional da instância funde operações pequenas de E/S em uma operação maior antes de passá-las ao Amazon EBS.

Se sua workload usar E/S sequenciais em volumes `st1` e `sc1` baseados em HDD, será possível ter um número de IOPS superior ao esperado conforme medido dentro de sua instância. Isso acontece quando o sistema operacional da instância funde operações de E/S sequenciais e as conta em unidades de 1.024 KiB. Se sua workload usar operações de E/S pequenas ou aleatórias, será possível ter uma throughput menor do que o esperado. Isso porque nós contamos cada E/S aleatória, não sequencial, para a contagem total de IOPS, que podem levá-lo a atingir o limite de volume de IOPS mais cedo do que o esperado.

Seja qual for o tipo de volume do EBS, se a IOPS ou a throughput não forem conforme o esperado de acordo com a configuração, garanta que a largura de banda da instância do EC2 não seja o fator limitante. Você sempre deve usar uma instância otimizada para EBS da geração atual (ou uma que inclua a conectividade de rede 10 Gb/s) para a performance ideal. Outra causa possível para a ausência da IOPS prevista é que você não está conduzindo E/S suficientes para volumes do EBS.

Monitore as características de E/S usando CloudWatch

Você pode monitorar essas características de E/S com as métricas de volume de cada CloudWatch volume. Métricas importantes a serem consideradas incluem o seguinte:

- `VolumeStalledIOCheck`
- `BurstBalance`

- `VolumeReadBytes` | `VolumeWriteBytes`
- `VolumeReadOps` | `VolumeWriteOps`
- `VolumeQueueLength`

`VolumeStalledIOCheck` monitora o status dos volumes do EBS para determinar quando eles estão danificados. A métrica é um valor binário que retornará um status `0` (aprovado) ou `1` (reprovado) dependendo do volume do EBS poder ou não realizar as operações de E/S. Essa verificação detecta problemas subjacentes na infraestrutura do Amazon EBS, como os seguintes:

- Problemas de hardware ou software nos subsistemas de armazenamento subjacentes aos volumes do EBS
- Problemas de hardware no host físico que afetam a acessibilidade dos volumes do EBS a partir da instância do EC2
- Problemas de conectividade entre a instância e os volumes do EBS

Se a `VolumeStalledIOCheck` métrica falhar, você pode esperar AWS para resolver o problema ou tomar medidas, como substituir o volume afetado ou interromper e reiniciar a instância à qual o volume está conectado. Na maioria dos casos, quando essa métrica falha, o EBS diagnostica e recupera automaticamente o volume em alguns minutos. Você pode usar a ação Pausar I/O AWS Fault Injection Service para executar experimentos controlados para testar sua arquitetura e monitoramento com base nessa métrica para melhorar sua resiliência a falhas de armazenamento.

Você pode medir a latência de E/S do armazenamento do Amazon EBS usando `VolumeReadOps`, `VolumeWriteOps`, `VolumeTotalReadTime` e `VolumeTotalWriteTime`. Você pode usar a expressão a seguir para monitorar a latência média de E/S do seu volume:

```
Average I/O latency in ms/op = (VolumeTotalReadTime + VolumeTotalWriteTime) /
 (VolumeReadOps + VolumeWriteOps)
```

Se a latência de E/S for maior de que você precisa, verifique o IOPS gerado para se certificar de que a aplicação não está tentando gerar mais IOPS do que você provisionou. Você pode usar a expressão a seguir para monitorar o IOPS médio gerado no volume:

```
Estimated average IOPS in ops/s = (Sum(VolumeReadOps) + Sum(VolumeWriteOps)) / (Period
 - Sum(VolumeIdleTime))
```

Se a aplicação exigir um número de IOPS maior do que seu volume pode fornecer, será necessário considerar usar um dos seguintes:

- Um volume `gp3`, `io2` ou `io1` que seja provisionado com IOPS suficientes para atingir a latência necessária
- Um volume `gp2` maior que forneça performance de IOPS de base suficiente

Os volumes `st1` e `sc1` baseados em HDD são projetados para ter performance melhor com workloads que aproveitam o tamanho de E/S máximo de 1.024 KiB. Para determinar o tamanho médio de E/S de seu volume, divida `VolumeWriteBytes` por `VolumeWriteOps`. O mesmo cálculo se aplica a operações de leitura. Se o tamanho de E/S médio ficar abaixo de 64 KiB, aumentando o tamanho de operações de E/S enviadas para um volume `st1` ou `sc1` o volume deve melhorar a performance.

> **Note**
>
> Se o tamanho médio de E/S for igual ou próximo de 44 KiB, será possível usar uma instância ou um kernel sem suporte para descritores indiretos. Qualquer kernel do Linux versão 3.8 ou posterior tem esse suporte, bem como qualquer instância da geração atual.

`BurstBalance` exibe o saldo do bucket de intermitência para os volumes `gp2`, `st1` e `sc1` como um porcentual do saldo restante. Quando seu bucket de intermitência é esgotado, a E/S de volume (para volumes `gp2`) ou a throughput de volume (para volumes `st1` e `sc1`) são limitadas à linha de base. Verifique o valor `BurstBalance` para determinar se seu volume está sendo limitado por esse motivo. Para obter uma lista completa das métricas do Amazon EBS disponíveis, consulte CloudWatch Métricas da Amazon para Amazon EBS e Métricas do Amazon EBS para instâncias baseadas Nitro.

Recursos relacionados

Para obter mais informações sobre as características de E/S do Amazon EBS, consulte a seguinte apresentação re:Invent: Amazon EBS: Como projetar visando a performance.

Inicializar volumes de Amazon EBS

Os volumes vazios do EBS recebem a performance máxima no momento em que são criados e não requerem inicialização (antes conhecida como pré-aquecimento).

Para volumes de qualquer tipo que foram criados de snapshots, os blocos de armazenamento devem ser extraídos do Amazon S3 e gravados no volume para poderem ser acessados. Essa ação preliminar leva tempo e pode causar um aumento significativo na latência de operações de E/S na primeira vez que cada bloco for acessado. A performance do volume é obtida depois que todos os blocos forem obtidos por download e gravados no volume.

> **Important**
>
> Durante a inicialização dos volumes de Provisioned IOPS SSD que foram criados de snapshots, a performance do volume pode ser reduzida para menos de 50% de seu nível esperado, o que faz com que o volume exiba um estado de `warning` na verificação do status de I/O Performance (Performance de E/S). Isso é esperado, e é possível ignorar o estado de `warning` em volumes de Provisioned IOPS SSD enquanto estiver inicializando esses volumes. Para obter mais informações, consulte Verificações de status do volume do EBS.

Para a maioria das aplicações, é aceitável a amortização do custo de inicialização ao longo da vida útil do volume. Para evitar essa ocorrência de performance inicial em um ambiente de produção, é possível usar uma das seguintes opções:

- Forçar a inicialização imediata do volume inteiro. Para obter mais informações, consulte Instâncias do Linux (instâncias do Linux) ou Instâncias do Windows (instâncias do Windows).
- Habilite as restauração rápida em um snapshot para garantir que os volumes do EBS criados de um snapshot sejam totalmente inicializados na criação e entreguem instantaneamente toda a sua performance provisionada. Para ter mais informações, consulte Restauração rápida de snapshots do Amazon EBS.

Instâncias do Linux

Como inicializar um volume criado de um snapshot no Linux

1. Anexe o volume recentemente restaurado à sua instância do Linux.
2. Use o comando lsblk para relacionar os dispositivos de blocos em sua instância.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvdf  202:80   0  30G  0 disk
```

```
xvda1 202:1    0   8G  0 disk /
```

Aqui é possível ver que o volume novo `/dev/xvdf`, está anexado, mas não montado (porque não há caminho listado na coluna `MOUNTPOINT`).

3. Use os utilitários dd ou fio para ler todos os blocos do dispositivo. O comando dd é instalado por padrão em sistemas Linux, mas fio é consideravelmente mais rápido porque permite leituras encadeadas várias vezes.

> **Note**
>
> Essa etapa pode levar de vários minutos a várias horas, dependendo da largura de banda da instância do EC2, das IOPS provisionadas para o volume e do tamanho do volume.

[dd] O parâmetro `if` (arquivo de entrada) deve ser configurado na unidade que você deseja inicializar. O parâmetro `of` (arquivo de saída) deve ser definido no dispositivo virtual nulo do Linux, `/dev/null`. O parâmetro `bs` define o tamanho do bloco da operação de leitura. Para a performance ideal, ele deve ser definido como 1 MB.

> **Important**
>
> O uso incorreto de dd pode destruir facilmente os dados de um volume. Não deixe de seguir precisamente o comando de exemplo abaixo. Somente o parâmetro `if=/dev/xvdf` irá variar dependendo do nome do dispositivo que você está lendo.

```
[ec2-user ~]$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

[fio] Se o fio estiver instalado em seu sistema, use o seguinte comando para inicializar seu volume. O parâmetro `--filename` (arquivo de entrada) deve ser configurado na unidade que você deseja inicializar.

```
[ec2-user ~]$ sudo fio --filename=/dev/xvdf --rw=read --bs=1M --iodepth=32 --
ioengine=libaio --direct=1 --name=volume-initialize
```

Use o comando a seguir para instalar o fio em Amazon Linux:

```
sudo yum install -y fio
```

Para instalar fio no Ubuntu, use o seguinte comando:

```
sudo apt-get install -y fio
```

Quando a operação for concluída, você verá um relatório da operação de leitura. Seu volume agora está pronto para uso. Para ter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso.

Instâncias do Windows

Antes de usar uma ou outra ferramenta, colete informações sobre os discos no sistema como se segue:

Para reunir informações sobre os discos do sistema

1. Use o comando wmic para listar os discos disponíveis no sistema:

```
wmic diskdrive get size,deviceid
```

A seguir está um exemplo de saída:

```
DeviceID            Size
\\.\PHYSICALDRIVE2  80517265920
\\.\PHYSICALDRIVE1  80517265920
\\.\PHYSICALDRIVE0  128849011200
\\.\PHYSICALDRIVE3  107372805120
```

2. Identifique o disco para inicializar usando dd ou fio. A unidade `C:` está em `\\.\PHYSICALDRIVE0`. É possível usar o utilitário `diskmgmt.msc` para comparar letras de unidades com números de unidades de disco, se não tiver certeza de que número de unidade usar.

Use the dd utility

Conclua os seguintes procedimentos para instalar e usar dd para inicializar um volume.

Considerações importantes

- A inicialização do volume leva de vários minutos a várias horas, dependendo da largura de banda da instância do EC2, das IOPS provisionadas para o volume e do tamanho do volume.
- O uso incorreto de dd pode destruir facilmente os dados de um volume. Certifique-se de seguir este procedimento com precisão.

Instalar dd para Windows

O programa dd para Windows fornece uma experiência semelhante ao programa dd que é geralmente disponível para sistemas Linux e Unix, e permite que você inicialize volumes do Amazon EBS que foram criados de snapshots. As versões beta mais recentes suportam o dispositivo `/dev/null` virtual. Se você instalar uma versão anterior, é possível usar o dispositivo `nul` virtual em vez disso. A documentação completa está disponível em http://www.chrysocome.net/dd.

1. Faça download da versão binária mais recente do dd para Windows em http://www.chrysocome.net/dd.
2. (Opcional) Crie uma pasta para utilitários de linha de comando que seja fácil de localizar e recordar, como `C:\bin`. Se você já tiver uma pasta designada para utilitários de linha de comando, poderá usar essa pasta na etapa a seguir.
3. Descompacte o pacote binário e copie o arquivo `dd.exe` para sua pasta de utilitários de linha de comando (por exemplo, `C:\bin`).
4. Adicione a pasta de utilitários de linha de comando à variável de ambiente de caminho para que você possa executar os programas nessa pasta de qualquer lugar.
   a. Escolha Iniciar, abra o menu de contexto (clique com o botão direito) de Computador e escolha Propriedades.
   b. Escolha Configurações avançadas de sistema, Variáveis de Ambiente.
   c. Em Variáveis de Sistema, selecione a variável Caminho e escolha Editar.
   d. Em Valor da variável, adicione um ponto e vírgula e o local de sua pasta de utilitário de linha de comando (**`;C:\bin\`**) no final do valor existente.
   e. Escolha OK para fechar a janela Editar Variável de Sistema.
5. Abra uma nova janela do prompt de comando. As seguintes etapas não atualizam as variáveis ambientais nas janelas de prompt de comando atuais. As janelas de prompt de comando que você abre agora que você concluiu a etapa anterior são atualizadas.

Inicializar um volume usando dd para Windows

Execute o seguinte comando para ler todos os blocos no dispositivo especificado (e envie a saída para o dispositivo virtual `/dev/null`). Este comando inicializa com segurança os dados existentes.

```
dd if=\\.\PHYSICALDRIVEn of=/dev/null bs=1M --progress --size
```

Pode haver um erro se dd tentar ler além do fim do volume. É possível ignorar isso com segurança.

Se você usou uma versão anterior do comando dd, ele não suporta o dispositivo `/dev/null`. Em vez disso, é possível usar o dispositivo `nul` da seguinte forma.

```
dd if=\\.\PHYSICALDRIVEn of=nul bs=1M --progress --size
```

Use the fio utility

Conclua os seguintes procedimentos para instalar e usar fio para inicializar um volume.

Como instalar fio para Windows

O programa fio para Windows fornece uma experiência semelhante ao programa fio que é geralmente disponível para sistemas Linux e Unix, e permite que você inicialize volumes do Amazon EBS criados de snapshots. Para obter mais informações, consulte https://github.com/axboe/fio.

1. Faça o download do instalador fio MSI ao expandir Ativos para a versão mais recente e selecionando o instalador MSI.
2. Instalar o fio.

Como inicializar um volume usando fio para Windows

1. Execute um comando semelhante ao seguinte para inicializar um volume:

```
fio --filename=\\.\PHYSICALDRIVEn  --rw=read --bs=128k --iodepth=32 --direct=1
 --name=volume-initialize
```

2. Quando a operação for concluída, você estará pronto para usar o novo volume. Para ter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso.

Configuração do Amazon EBS e RAID

Com o Amazon EBS, é possível usar qualquer uma das configurações padrão RAID que é possível usar com um servidor bare metal tradicional, desde que essa configuração RAID específica tenha suporte no sistema operacional para sua instância. A razão disso é que todo o RAID é realizado no nível do software.

Os dados dos volumes do Amazon EBS são replicados em vários servidores em uma zona de disponibilidade para evitar perdas de dados causadas por falha em qualquer componente único. Essa replicação torna os volumes do Amazon EBS 10 vezes mais confiável do que as unidades de disco típicas. Para obter mais informações, consulte Disponibilidade e durabilidade do Amazon EBS nas páginas de detalhes do produto Amazon EBS.

Conteúdo

Opções de configuração de RAID

Criar uma matriz de RAID 0 permite atingir um nível de performance para um sistema de arquivos maior do que é possível provisionar em um único volume Amazon EBS. Use RAID 0 quando a performance de E/S for da máxima importância. Com o RAID 0, a E/S é distribuída entre os volumes em uma distribuição. Se você adicionar um volume, obterá a adição direta de throughput e IOPS. No entanto, lembre-se de que a performance da distribuição é limitada ao volume de pior performance do conjunto e que a perda de um único volume do conjunto resulta em perda de dados completa para a matriz.

O tamanho resultante de uma matriz de RAID 0 é a soma dos tamanhos dos volumes nela, e a largura de banda é a soma da largura de banda dos volumes nela. Por exemplo, dois volumes `io1` de 500 GiB, com 4.000 IOPS provisionadas cada, criarão uma matriz RAID 0 de 1.000 GiB com uma largura de banda disponível de 8.000 IOPS e 1.000 MiB/s de throughput.

> **Important**
>
> O RAID 5 e o RAID 6 não são recomendados para o Amazon EBS porque as operações de gravação de paridade desses modos de RAID consomem um pouco do IOPS disponível para

os seus volumes. Dependendo da configuração de sua matriz de RAID, esses modos de RAID fornecem de 20 a 30% menos IOPS útil do que uma configuração de RAID 0. O maior custo também é um fator nesses modos de RAID; ao usar tamanhos e velocidades idênticos de volume, uma matriz de RAID 0 de 2 volumes pode superar uma matriz de RAID 6 de 4 volumes que custa duas vezes mais.
Também não se recomenda o uso do RAID 1 com o Amazon EBS. O RAID 1 exige mais largura de banda do Amazon EC2 para o Amazon EBS do que nas configurações sem RAID, pois os dados são gravados em vários volumes simultaneamente. Além disso, o RAID 1 não fornece nenhuma melhoria na performance de gravação.

Criar uma matriz RAID 0

Use o procedimento a seguir para criar a matriz RAID 0.

Considerações

- Antes de executar esse procedimento, é necessário decidir o tamanho que sua matriz RAID 0 deve ter e quantas IOPS você deseja provisionar.
- Crie volumes com valores de performance de IOPS e tamanho idênticos para sua matriz. Certifique-se de não criar uma matriz que exceda a largura de banda disponível de sua instância do EC2.
- É necessário evitar inicializar a partir de um volume RAID. Se uma falha em um dos dispositivos ocorrer, talvez você não consiga iniciar o sistema operacional.

Instâncias do Linux

Para criar uma matriz de RAID 0 no Linux

1. Crie os volumes do Amazon EBS para sua matriz. Para ter mais informações, consulte Crie um volume do Amazon EBS..
2. Anexe os volumes do Amazon EBS à instância na qual você deseja hospedar a matriz. Para obter mais informações, consulte Vincular um volume de Amazon EBS a uma instância.
3. Use o comando mdadm para criar um dispositivo RAID lógico dos volumes do Amazon EBS anexados recentemente. Substitua o número de volumes em sua matriz por *number_of_volumes* e os nomes dos dispositivos para cada volume na matriz (como `/dev/`

`xvdf`) por *`device_name`*. Também é possível substituir *`MY_RAID`* pelo seu próprio nome exclusivo para a matriz.

> **Note**
>
> É possível relacionar os dispositivos em sua instância com o comando lsblk para encontrar os nomes dos dispositivos.

Para criar uma matriz de RAID 0, execute o seguinte comando (observe a opção `--level=0` para distribuir a matriz):

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --
raid-devices=number_of_volumes device_name1 device_name2
```

> **Tip**
>
> Se você receber o erro `mdadm: command not found`, use o seguinte comando para instalar o mdadm:`sudo yum install mdadm`.

4. Reserve tempo para a matriz de RAID ser inicializada e sincronizada. É possível acompanhar o progresso dessas operações com o seguinte comando:

```
[ec2-user ~]$ sudo cat /proc/mdstat
```

A seguir está um exemplo de saída:

```
Personalities : [raid0]
md0 : active raid0 xvdc[1] xvdb[0]
      41910272 blocks super 1.2 512k chunks

unused devices: <none>
```

Em geral, é possível exibir informações detalhadas sobre sua matriz de RAID com o seguinte comando:

```
[ec2-user ~]$ sudo mdadm --detail /dev/md0
```

A seguir está um exemplo de saída:

```
/dev/md0:
           Version : 1.2
     Creation Time : Wed May 19 11:12:56 2021
        Raid Level : raid0
        Array Size : 41910272 (39.97 GiB 42.92 GB)
      Raid Devices : 2
     Total Devices : 2
       Persistence : Superblock is persistent

       Update Time : Wed May 19 11:12:56 2021
             State : clean
    Active Devices : 2
   Working Devices : 2
    Failed Devices : 0
     Spare Devices : 0

        Chunk Size : 512K

Consistency Policy : none

              Name : MY_RAID
              UUID : 646aa723:db31bbc7:13c43daf:d5c51e0c
            Events : 0

    Number   Major   Minor   RaidDevice State
       0     202       16        0      active sync   /dev/sdb
       1     202       32        1      active sync   /dev/sdc
```

5. Crie um sistema de arquivos em sua matriz de RAID e forneça a esse sistema de arquivos uma identificação para usar quando ao montá-lo posteriormente. Por exemplo, para criar um sistema de arquivos ext4 com a identificação *MY_RAID*, execute o seguinte comando:

```
[ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
```

Dependendo dos requisitos da aplicação ou das limitações do sistema operacional, é possível usar um tipo diferente de sistema de arquivos, como ext3 ou XFS (consulte a documentação do sistema de arquivos para saber o comando de criação de sistema de arquivos correspondente).

6. Para garantir que a matriz de RAID seja remontada automaticamente na inicialização, crie um arquivo de configuração para conter informações de RAID:

```
[ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
```

> **Note**
>
> Se você estiver usando uma distribuição do Linux que não seja o Amazon Linux, talvez seja necessário modificar esse comando. Por exemplo, talvez seja necessário colocar o arquivo em outro local, ou talvez seja necessário adicionar o parâmetro `--examine`. Para obter mais informações, execute man mdadm.conf em sua instância do Linux.

7. Crie uma nova imagem de ramdisk para pré-carregar corretamente os módulos de dispositivo de bloco para sua nova configuração de RAID:

```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. Crie um ponto de montagem para sua matriz RAID.

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

9. Finalmente, monte o dispositivo RAID no ponto de montagem que você criou:

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

O dispositivo RAID agora está pronto para uso.

10. (Opcional) Para montar esse volume do Amazon EBS em cada reinicialização do sistema, adicione uma entrada para o dispositivo ao arquivo `/etc/fstab`.

    a. Crie um backup do seu arquivo `/etc/fstab` para usar se você destruir ou excluir acidentalmente esse arquivo quando for editar.

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

    b. Abra o arquivo `/etc/fstab` usando seu editor de texto favorito, como nano ou vim.

    c. Comente todas as linhas que começam com "`UUID=`" e, no final do arquivo, adicione uma nova linha para o volume de RAID usando o seguinte formato:

```
device_label mount_point file_system_type fs_mntops fs_freq fs_passno
```

Os três últimos campos dessa linha são as opções de montagem do sistema de arquivos, a frequência de despejo do sistema de arquivos e a ordem das verificações do sistema de arquivos feitas no momento da inicialização. Se você não souber quais valores devem ser, use os valores no exemplo abaixo (`defaults,nofail 0 2`). Para obter mais informações sobre `/etc/fstab`, consulte a página fstab do manual (inserindo man fstab na linha de comando). Por exemplo, para montar o sistema de arquivos ext4 no dispositivo com a identificação MY_RAID no ponto de montagem `/mnt/raid`, adicione a seguinte entrada a `/etc/fstab`.

> **Note**
>
> Se você pretende inicializar sua instância sem esse volume anexado (por exemplo, para que esse volume possa ser movido entre instâncias diferentes), adicione a opção de montagem `nofail` que permite à instância ser inicializada mesmo se houver erros na montagem do volume. Os derivados de Debian, como o Ubuntu, também devem adicionar a opção de montagem `nobootwait`.

```
LABEL=MY_RAID       /mnt/raid   ext4    defaults,nofail        0       2
```

d. Depois de adicionar a nova entrada a `/etc/fstab`, você precisa verificar se a sua entrada funciona. Execute o comando sudo mount -a para montar todos os sistemas de arquivos em `/etc/fstab`.

```
[ec2-user ~]$ sudo mount -a
```

Se o comando anterior não produzir um erro, o arquivo `/etc/fstab` será válido e o sistema de arquivos será montado automaticamente na próxima inicialização. Se o comando produzir erros, examine-os e tente corrigir seu `/etc/fstab`.

> **Warning**
>
> Erros no arquivo `/etc/fstab` podem impedir a inicialização de um sistema. Não desative um sistema que tenha erros no arquivo `/etc/fstab`.

e. (Opcional) Se você não souber corrigir os erros no `/etc/fstab`, sempre poderá restaurar seu arquivo `/etc/fstab` de backup com o seguinte comando.

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

Instâncias do Windows

Para criar uma matriz de RAID 0 no Windows

1. Crie os volumes do Amazon EBS para sua matriz. Para ter mais informações, consulte Crie um volume do Amazon EBS..
2. Anexe os volumes do Amazon EBS à instância na qual você deseja hospedar a matriz. Para obter mais informações, consulte Vincular um volume de Amazon EBS a uma instância.
3. Conecte-se à sua instância do Windows. Para obter mais informações, consulte Conectar-se à sua instância do Windows.
4. Abra um prompt de comando e digite o comando diskpart.

```
diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-BM6QPPL51CO
```

5. No prompt `DISKPART`, liste os discos disponíveis com o seguinte comando.

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B
  Disk 2    Online            8 GB      0 B
```

Identifique os discos que deseja usar em sua matriz e anote os números dos discos.

6. Cada disco que deseja usar em sua matriz deve ser um disco dinâmico online que não contenha nenhum volume existente. Use as seguintes etapas para converter discos básicos em discos dinâmicos e excluir todos os volumes existentes.

   a. Selecione um disco que deseja usar em sua matriz com o seguinte comando, substituindo *n* pelo número do disco.

```
DISKPART> select disk n

Disk n is now the selected disk.
```

   b. Se o disco selecionado estiver listado como `Offline`, deixe-o online executando o comando online disk.

   c. Se o disco selecionado não tiver um asterisco na coluna `Dyn` na saída do comando list disk anterior, você precisará convertê-lo em um disco dinâmico.

```
DISKPART> convert dynamic
```

> **Note**
>
> Se você receber um erro de que o disco é protegido contra gravação, desmarque o sinalizador de somente leitura no comando ATTRIBUTE DISK CLEAR READONLY e tente novamente a conversão do disco dinâmico.

   d. Use o comando detail disk para verificar se há volumes existentes no disco selecionado.

```
DISKPART> detail disk

XENSRC PVDISK SCSI Disk Device
Disk ID: 2D8BF659
Type   : SCSI
Status : Online
Path   : 0
Target : 1
LUN ID : 0
Location Path : PCIROOT(0)#PCI(0300)#SCSI(P00T01L00)
Current Read-only State : No
Read-only  : No
```

```
Boot Disk   : No
Pagefile Disk   : No
Hibernation File Disk   : No
Crashdump Disk   : No
Clustered Disk   : No

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 2     D   NEW VOLUME   FAT32  Simple      8189 MB  Healthy
```

Anote todos os números de volumes no disco. Neste exemplo, o número do volume é 2. Se não houver volumes, ignore a próxima etapa.

e. (Necessário somente se foram encontrados volumes na etapa anterior) Selecione e exclua todos os volumes existentes no disco que você identificou na etapa anterior.

> **Warning**
>
> Isso destrói todos os dados existentes no volume.

i. Selecione o volume, substituindo *n* pelo número do volume.

```
DISKPART> select volume n
Volume n is the selected volume.
```

ii. Exclua o volume.

```
DISKPART> delete volume

DiskPart successfully deleted the volume.
```

iii. Repita essas subetapas para cada volume que você precisa excluir no disco selecionado.

f. Repita Step 6 para cada disco que deseja usar em sua matriz.

7. Verifique se os discos que você deseja usar agora são dinâmicos. Nesse caso, estamos usando discos 1 e 2 para o volume RAID.

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
```

```
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B   *
  Disk 2    Online            8 GB      0 B   *
```

8. Crie a matriz de RAID. No Windows, um volume de RAID 0 é referido como um volume distribuído.

   Para criar uma matriz de volume distribuído nos discos 1 e 2, use o seguinte comando (observe a opção `stripe` para distribuir a matriz):

```
DISKPART> create volume stripe disk=1,2
DiskPart successfully created the volume.
```

9. Verifique seu novo volume.

```
DISKPART> list volume

  DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     C                NTFS   Partition     29 GB  Healthy    System
  Volume 1                      RAW    Stripe        15 GB  Healthy
```

   Observe que a coluna `Type` agora indica que o Volume 1 é um volume `stripe`.

10. Selecione e formate seu volume para que você possa começar a usá-lo.

    a. Selecione o volume que você deseja formatar, substituindo *n* pelo número do volume.

```
DISKPART> select volume n

Volume n is the selected volume.
```

    b. Formate o volume.

> **Note**
>
> Para executar uma formatação completa, omita a opção `quick`.

```
DISKPART> format quick recommended label="My new volume"

  100 percent completed

DiskPart successfully formatted the volume.
```

c. Atribua uma letra de unidade disponível ao seu volume.

```
DISKPART> assign letter f

DiskPart successfully assigned the drive letter or mount point.
```

Seu novo volume agora está pronto para uso.

Criar snapshots de volumes em uma matriz RAID

Se você deseja fazer backup dos dados nos volumes do EBS em um array RAID usando snapshots, verifique se os snapshots estão consistentes. Isso ocorre porque os snapshots desses volumes são criados de maneira independente. Restaurar os volumes do EBS em uma matriz RAID de snapshots que não estão sincronizados prejudicaria a integridade da matriz.

Para criar um conjunto consistente de snapshots para a matriz RAID, use snapshots de vários volumes do EBS. Os instantâneos de vários volumes permitem que você tire point-in-time instantâneos coordenados com dados e consistentes em falhas em vários volumes do EBS conectados a uma instância do EC2. Não é necessário interromper a instância para coordenar entre volumes a fim de garantir consistência, pois os snapshots são tirados automaticamente em vários volumes do EBS. Para obter mais informações, consulte as etapas para criar snapshots de vários volumes em Criar snapshots do Amazon EBS.

Comparar volumes do EBS

É possível testar a performance dos volumes do Amazon EBS simulando workloads de E/S. O processo é o seguinte:

1. Execute uma instância otimizada para EBS.
2. Crie novos volumes do EBS.

3. Anexe os volumes à sua instância otimizada para EBS.
4. Configure e monte o dispositivo de blocos.
5. Instale uma ferramenta para comparar a performance de E/S.
6. Compare a performance de E/S de seus volumes.
7. Exclua os volumes e encerre sua instância para não continuar a ser cobrado.

> **Important**
>
> Alguns procedimentos resultam na destruição de dados existentes em volumes do EBS que você compara. Os procedimentos de comparação são destinados ao uso em volumes criados especialmente para fins de teste, não volumes de produção.

Configurar a instância

Para obter a performance ideal em volumes do EBS, recomendamos que você use uma instância otimizada para EBS. As instâncias otimizadas para EBS fornecem throughput dedicada entre o Amazon EC2 e o Amazon EBS, com instância. As instâncias otimizadas para EBS fornecem largura de banda dedicada entre o Amazon EC2 e o Amazon EBS, com especificações que dependem do tipo de instância.

Para criar uma instância otimizada para EBS, escolha Iniciar como instância otimizada para EBS ao executar a instância usando o console do Amazon EC2 ou especifique --ebs-optimized ao utilizar a linha de comando. Certifique-se de selecionar um tipo de instância que ofereça suporte a essa opção.

Configurar volumes de Provisioned IOPS SSD ou Finalidade geral (SSD)

Para criar volumes SSD de IOPS provisionadas (`io1` e `io2`) ou SSD de uso geral (`gp2` e `gp3`) usando o console do Amazon EC2, em Volume type (Tipo de volume), escolhaProvisioned IOPS SSD (io1) (SSD de IOPS provisionadas (io1)), Provisioned IOPS SSD (io2) (SSD de IOPS provisionadas (io2)), General Porpose SSD (gp2) (SSD de uso geral (gp2)) ou General Purpose SSD (gp3) (SSD de uso geral (gp3)). Na linha de comando, especifique `io1`, `io2`, `gp2` ou `gp3` para o parâmetro --volume-type. Para os volumes de `io1`, `io2`, e `gp3`, especifique o número de operações de E/S por segundo (IOPS) para o parâmetro --iops. Para obter mais informações, consulte Tipos de volume do Amazon EBS e Crie um volume do Amazon EBS..

(Somente para instâncias do Linux) Para os testes de exemplo, recomendamos criar uma matriz RAID 0 com 6 volumes para garantir um alto nível de performance. Como você será cobrado por gigabytes provisionados (e pelo número de IOPS provisionadas para volumes de io1, io2 e gp3), e não pelo número de volumes, não há nenhum custo adicional para criar vários volumes menores e utilizá-los para criar um conjunto de stripes. Se você estiver utilizando o Oracle Orion para comparar seus volumes, ele poderá simular a segmentação da mesma forma que o ASM do Oracle; portanto, recomendamos que você deixe a segmentação a cargo do Orion. Se você estiver usando uma ferramenta de comparação diferente, precisará fazer o stripe de volumes por conta própria.

Para obter mais informações sobre como criar uma matriz RAID 0, consulte Criar uma matriz RAID 0.

Configurar volumes HDD otimizado para throughput (**`st1`**) ou HDD a frio (**`sc1`**)

Para criar um volume `st1`, escolha Throughput Optimized HDD (HDD otimizado para throughput) ao criar o volume usando o console do Amazon EC2 ou especifique --type **`st1`** ao usar a linha de comando. Para criar um volume `sc1`, escolha Cold HDD (HDD a frio) ao criar o volume usando o console do Amazon EC2 ou especifique --type **`sc1`** ao usar a linha de comando. Para obter informações sobre a criação de volumes do EBS, consulte Crie um volume do Amazon EBS.. Para obter informações sobre como anexar esses volumes à sua instância, consulte Vincular um volume de Amazon EBS a uma instância.

(somente instâncias Linux) AWS fornece um modelo JSON para uso AWS CloudFormation que simplifica esse procedimento de configuração. Acesse o modelo e salve-o como um arquivo JSON. AWS CloudFormation permite que você configure suas próprias chaves SSH e oferece uma maneira mais fácil de configurar um ambiente de teste de desempenho para avaliar `st1` volumes. O modelo cria uma instância de geração atual e um volume `st1` de 2 TiB e anexa o volume à instância em `/dev/xvdf`.

(Somente instâncias do Linux) Para criar um volume de HDD usando o modelo

1. Abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.
2. Selecione Criar Stack.
3. Escolha Upload a Template to Amazon S3 e selecione o modelo JSON que você obteve anteriormente.
4. Dê um nome para a pilha como “ebs-perf- testes” e selecione um tipo de instância (o padrão é r3.8xlarge) e a chave SSH.
5. Selecione Next duas vezes e, em seguida, escolha Create Stack.

6. Depois que o status da sua nova pilha passar de CREATE_IN_PROGRESS (Criação em andamento) para COMPLETE (Concluído), escolha Outputs (Saídas) para obter a entrada de DNS público para sua nova instância, que terá um volume `st1` de 2 TiB anexado a ela.
7. Usando SSH, conecte-se à nova pilha como usuário **`ec2-user`**, com o nome de host obtido da entrada de DNS na etapa anterior.
8. Vá para Instalar ferramentas de comparação.

Instalar ferramentas de comparação

A tabela a seguir lista algumas das ferramentas que é possível usar para comparar a performance de volumes do EBS.

Instâncias do Linux

Ferramenta	Descrição

fio	Para comparar a performance de E/S. Observe que fio tem uma dependência sobre `libaio-devel` .
	
	Execute o comando a seguir para instalar o fio no Amazon Linux:
	
	`[ec2-user ~]$ sudo yum install -y fio`
	
	Para instalar fio no Ubuntu, execute o seguinte comando:
	
	`sudo apt-get install -y fio`

Ferramenta de calibração do Oracle Orion	Para calibrar a performance de E/S de sistemas de armazenamento a serem usados com bancos de dados do Oracle.

Instâncias do Windows

Ferramenta	Descrição
DiskSpd	DiskSpd é uma ferramenta de desempenho de armazenamento das equipes de engenharia de infraestrutura do Windows, Windows Server e Cloud Server da Microsoft. Disponível para download em https://github.com/Microsoft/diskspd/releases. Depois de fazer download do arquivo executável `diskspd.exe` , abra um prompt de comando com direitos administrativos (escolhendo “Executar como administrador”) e navegue até o diretório onde você copiou o arquivo `diskspd.exe` . Copie o arquivo executável `diskspd.exe` desejado da pasta executável apropriada, `amd64fre`, `armfre` ou `x86fre`) para um caminho curto e simples, como `C:\DiskSpd` . Na maioria dos casos, você desejará a versão de 64 bits DiskSpd do da `amd64fre` pasta. O código-fonte do DiskSpd está hospedado GitHub em: https://github.com/Microsoft/diskspd.
CrystalDiskMark	CrystalDiskMark é um software simples de benchmark de disco. Ele está disponível para download em https://crystalmark.info/en/software/crystaldiskmark/.

Essas ferramentas de avaliação oferecem suporte a uma ampla variedade de parâmetros de teste. Use os comandos que aproximam workloads às quais seus volumes oferecerão suporte. Os comandos fornecidos abaixo servem como exemplos para ajudá-lo a começar a usar.

Escolha o comprimento da fila de volume

Escolha do melhor comprimento da fila de volume com base em sua workload e tipo de volume.

Tamanho da fila em volumes baseados em SSD

Para determinar o tamanho ideal da fila para sua workload em volumes baseados em SSD, recomendamos focar em um tamanho da fila de 1 para cada 1.000 IOPS disponíveis (linha de base para volumes de Finalidade geral (SSD) e a quantidade provisionada para volumes de Provisioned

IOPS SSD). Depois, é possível monitorar a performance de sua aplicação e ajustar esse valor com base nos requisitos da aplicação.

Aumentar o comprimento da fila é benéfico até que você atinja as IOPS provisionadas, a throughput ou o valor ideal de comprimento da fila de sistema, que é atualmente configurado como 32. Por exemplo, para um volume com 3.000 IOPS provisionadas deve-se ter como meta um comprimento de fila 3. É necessário experimentar ajustar esses valores para cima ou para baixo para ver qual funciona melhor para sua aplicação.

Tamanho da fila em volumes baseados em HDD

Para determinar o tamanho ideal da fila para sua workload em volumes baseados em HDD, recomendamos que você foque em um comprimento da fila pelo menos 4 ao executar operações de E/S sequenciais de 1 MiB. Depois, é possível monitorar a performance de seu aplicativo e ajustar esse valor com base nos requisitos do aplicativo. Por exemplo, um volume `st1` de 2 TiB com throughput de intermitência de 500 MiB/s e IOPS de 500 deve focar em um comprimento da fila de 4, 8 ou de 16 ao executar operações de E/S sequenciais de 1.024 KiB, 512 KiB ou 256 KiB respectivamente. É necessário experimentar ajustar esses valores para cima ou para baixo e ver qual funciona melhor com sua aplicação.

Desabilitar estados C

Antes de executar a referência, desative os estados C do processador. Desativar os núcleos temporariamente em uma CPU compatível pode entrar em um estado C para economizar energia. Quando o núcleo é chamado para retomar o processamento, leva um determinado tempo até o núcleo voltar a funcionar por completo. Esta latência pode interferir nas rotinas de comparação do processador. Para obter mais informações sobre estados C e quais tipos de instância do EC2 são compatíveis a eles, consulte Controle de estado do processador para sua instância do EC2.

Instâncias do Linux

É possível desativar os estados C no Amazon Linux, RHEL e CentOS da seguinte maneira:

1. Obtenha o número de estados C.

```
$ C:\> cpupower idle-info | grep "Number of idle states:"
```

2. Desative os estados C de c1 a cN. De preferência, os núcleos devem estar no estado c0.

```
$ C:\> for i in `seq 1 $((N-1))`; do cpupower idle-set -d $i; done
```

Instâncias do Windows

É possível desativar os estados C no Windows da seguinte maneira:

1. Em PowerShell, obtenha o esquema de energia ativa atual.

```
$current_scheme = powercfg /getactivescheme
```

2. Obtenha o GUID do esquema de energia.

```
(Get-WmiObject -class Win32_PowerPlan -Namespace "root\cimv2\power" -Filter
 "ElementName='High performance'").InstanceID
```

3. Obtenha o GUID da configuração de energia.

```
(Get-WmiObject -class Win32_PowerSetting -Namespace "root\cimv2\power" -Filter
 "ElementName='Processor idle disable'").InstanceID
```

4. Obtenha o GUID do subgrupo da configuração de energia.

```
(Get-WmiObject -class Win32_PowerSettingSubgroup -Namespace "root\cimv2\power" -
Filter "ElementName='Processor power management'").InstanceID
```

5. Desative os estados C definindo o valor do índice como 1. Um valor igual a 0 indica que os estados C estão desativados.

```
powercfg /
setacvalueindex <power_scheme_guid> <power_setting_subgroup_guid> <power_setting_guid>
 1
```

6. Defina o esquema ativo para garantir que as configurações sejam salvas.

```
powercfg /setactive <power_scheme_guid>
```

Benchmarking de performance

Os seguintes procedimentos descrevem comandos de comparação para vários tipos de volumes do EBS.

Execute os seguintes comandos em uma instância otimizada para EBS com volumes do EBS anexados. Se os volumes do EBS tiverem sido criados de snapshots, inicialize-os antes do benchmarking. Para ter mais informações, consulte Inicializar volumes de Amazon EBS.

Após terminar de testar seus volumes, consulte os seguintes tópicos para obter ajuda para limpar: Excluir um volume de Amazon EBS e Encerrar a instância.

Avalie a performance dos volumes de Provisioned IOPS SSD e Finalidade geral (SSD)

Instâncias do Linux

Execute fio na matriz RAID 0 que você criou.

O seguinte comando executa operações de gravação aleatórias de 16 KB.

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_vol0 --ioengine=psync --
name fio_test_file --direct=1 --rw=randwrite --bs=16k --size=1G --numjobs=16 --
time_based --runtime=180 --group_reporting --norandommap
```

O seguinte comando executa operações de leitura aleatórias de 16 KB.

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_vol0 --name fio_test_file --direct=1
 --rw=randread --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --
group_reporting --norandommap
```

Para obter mais informações sobre como interpretar os resultados, consulte este tutorial: Inspeção de performance de E/S de disco com fio.

Instâncias do Windows

Execute DiskSpd no volume que você criou.

O comando a seguir executará um teste de E/S aleatório de 30 segundos usando um arquivo de teste de 20 GB localizado na unidade `C:`, com taxas de 25% de gravação e de 75% de leitura e um tamanho de bloco de 8 K. Ele usará oito threads de operador, cada um com quatro operações de E/S pendentes, e uma semente de valor de entropia de gravação de 1 GB. Os resultados do teste serão salvos em um arquivo de texto chamado `DiskSpeedResults.txt`. Esses parâmetros simulam uma workload OLTP do SQL Server.

```
diskspd -b8K -d30 -o4 -t8 -h -r -w25 -L -Z1G -c20G C:\iotest.dat > DiskSpeedResults.txt
```

Para obter mais informações sobre como interpretar os resultados, consulte este tutorial: Inspecionar a performance de E/S com o DiskSPd.

Benchmark de volumes **st1** e **sc1** (instâncias do Linux)

Execute fio em seu volume do `st1` ou `sc1`.

> **Note**
>
> Antes de executar esses testes, defina E/S em buffer na instância conforme descrito em Aumentar a leitura antecipada para workloads com muitas operações de leitura e alta throughput em `st1` e `sc1` (somente instâncias do Linux).

O seguinte comando executa operações de leitura sequenciais de 1 MiB em um dispositivo de blocos `st1` anexado (por exemplo, `/dev/xvdf`):

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=read --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_read_test
```

O seguinte comando executa operações de gravação sequenciais de 1 MiB em um dispositivo de blocos `st1` anexado:

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=write --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_write_test
```

Algumas workloads executam uma combinação de leituras e gravações sequenciais para diferentes partes de dispositivo de blocos. Para comparar essa workload, recomendamos que você use trabalhos de fio separados, simultâneos, para leituras e gravações, e use a opção fio `offset_increment` para focar em locais diferentes de dispositivo de blocos para cada trabalho.

Executar essa workload é um pouco mais complicado do que uma workload de gravação ou leitura sequenciais. Use um editor de texto para criar um arquivo de trabalho de fio, chamado de `fio_rw_mix.cfg` neste exemplo, que contém o seguinte:

```
[global]
clocksource=clock_gettime
```

```
randrepeat=0
runtime=180

[sequential-write]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=write
rwmixread=0
rwmixwrite=100

[sequential-read]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=read
rwmixread=100
rwmixwrite=0
offset=100g
```

Em seguida, execute o seguinte comando:

```
[ec2-user ~]$ sudo fio fio_rw_mix.cfg
```

Para obter mais informações sobre como interpretar os resultados, consulte este tutorial: Inspeção de performance de E/S de disco com fio.

Vários trabalhos de fio para E/S direta, mesmo que usando operações de leitura ou gravação sequenciais, podem resultar em uma throughput mais baixa do que o esperado para volumes `st1` e `sc1`. Recomendamos que você use um trabalho direto de E/S e use o parâmetro `iodepth` para controlar o número de operações simultâneas de E/S.

Amazon Data Lifecycle Manager

É possível usar o Amazon Data Lifecycle Manager para automatizar a criação, a retenção e a exclusão de snapshots do EBS e de AMIs apoiadas pelo EBS. Quando você automatiza o gerenciamento de snapshot e AMI, isso ajuda a:

- Proteger dados valiosos impondo uma programação regular de backup.
- Crie AMIs padronizadas que podem ser atualizadas em intervalos regulares.
- Reter os backups conforme exigido por auditores ou pelas regras de conformidade interna.
- Reduzir os custos de armazenamento ao excluir backup obsoletos.
- Criar políticas de backup de recuperação de desastres que fazem backup de dados em regiões ou contas isoladas.

Quando combinado com os recursos de monitoramento da Amazon EventBridge e do Amazon Data Lifecycle Manager AWS CloudTrail, o Amazon Data Lifecycle Manager fornece uma solução de backup completa para instâncias do Amazon EC2 e volumes individuais do EBS sem custo adicional.

> **Important**
>
> - O Amazon Data Lifecycle Manager não gerencia snapshots ou AMIs criados por qualquer outro meio.
> - O Amazon Data Lifecycle Manager não automatiza a criação, a retenção e a exclusão de AMIs baseadas em armazenamento de instância.

Conteúdo

- Monitorar o ciclo de vida de snapshots e AMIs
- Solução de problemas

Cotas

Sua AWS conta tem as seguintes cotas relacionadas ao Amazon Data Lifecycle Manager:

Descrição	Cota
Políticas personalizadas de ciclo de vida por região	100
Políticas padrão para snapshots do EBS por região	1
Políticas padrão para AMIs baseadas no EBS por região	1
Tags por recurso	45

Como Amazon Data Lifecycle Manager funciona

Veja a seguir os elementos de chaves do Amazon Data Lifecycle Manager.

Elementos

- Políticas
- Agendas da política (somente políticas personalizadas)
- Tags do recurso-alvo (somente políticas personalizadas)
- Snapshots
- AMIs apoiadas pelo EBS
- Tags do Amazon Data Lifecycle Manager

Políticas

Com o Amazon Data Lifecycle Manager, você cria políticas para definir os requisitos de criação e retenção de backup. Essas políticas geralmente especificam o seguinte:

- Tipo de política: define o tipo de recursos de backup que a política gerencia (snapshots ou AMIs baseadas no EBS).
- Recursos-alvo: define o tipo dos recursos que são alvo da política (instâncias ou volumes do EBS).
- Frequência de criação: define com que frequência a política é executada e cria snapshots ou AMIs.
- Limite de retenção: define por quanto tempo a política retém os snapshots ou as AMIs após sua criação.
- Ações adicionais: define as ações adicionais que a política deve realizar, como cópia entre regiões, arquivamento ou marcação de recursos.

O Amazon Data Lifecycle Manager oferece políticas padrão e políticas personalizadas.

Políticas padrão

As políticas padrão fazem backup de todos os volumes e instâncias em uma região que não têm backups recentes. Opcionalmente, você pode excluir volumes e instâncias especificando parâmetros de exclusão.

O Amazon Data Lifecycle Manager é compatível com as seguintes políticas padrão:

- Política padrão para snapshots do EBS: tem como alvo os volumes e automatiza a criação, a retenção e a exclusão de snapshots.
- Política padrão para AMIs baseadas no EBS: tem como alvo as instâncias e automatiza a criação, a retenção e o cancelamento do registro das AMIs baseadas no EBS.

Você só pode ter uma política padrão por tipo de recurso em cada conta e região da AWS .

Políticas personalizadas

As políticas personalizadas têm como alvo recursos específicos com base nas tags atribuídas a eles e são compatíveis com atributos avançados, como restauração rápida de snapshots, arquivamento de snapshots, cópia entre contas e scripts prévios e posteriores. Uma política personalizada pode incluir até quatro agendas, e cada agenda pode ter sua própria frequência de criação, limite de retenção e configuração avançada de atributos.

O Amazon Data Lifecycle Manager é compatível com as seguintes políticas personalizadas:

- Política de snapshots do EBS: tem como alvo os volumes ou as instâncias, e automatiza a criação, a retenção e a exclusão dos snapshots do EBS.
- Política de AMI baseada no EBS: tem como alvo as instâncias e automatiza a criação, a retenção e o cancelamento do registro das AMIs baseadas no EBS.
- Política de evento de cópia entre contas: automatiza ações de cópia entre regiões para os snapshots que são compartilhados com você.

Para ter mais informações, consulte Comparação entre políticas padrão e políticas personalizadas.

Agendas da política (somente políticas personalizadas)

As programações de política definem quando os snapshots ou AMIS são criados pela política. As políticas podem ter até quatro programações — uma obrigatória e até três opcionais.

Adicionar várias programações a uma única política permite que você crie snapshots ou AMIs em frequências diferentes usando a mesma política. Por exemplo, é possível criar uma única política que cria snapshots diários, semanais, mensais e anuais. Isso elimina a necessidade de gerenciar várias políticas.

Para cada programação, é possível definir a frequência, configurações de restauração rápida de snapshots (somente políticas de ciclo de vida do snapshot), regras de cópia entre regiões e tags. As etiquetas atribuídas a um agendamento são automaticamente atribuídas aos snapshots ou AMIs criados quando o agendamento é iniciado. Além disso, o Amazon Data Lifecycle Manager atribui automaticamente uma tag gerada pelo sistema com base na frequência da programação a cada snapshot ou AMI.

Cada agendamento é acionado individualmente com base na frequência. Se vários agendamentos forem iniciados ao mesmo tempo, o Amazon Data Lifecycle Manager criará apenas um snapshot ou uma AMI e aplicará as configurações de retenção do agendamento que tem o período de retenção mais alto. As etiquetas de todos os agendamentos iniciados são aplicadas ao snapshot ou à AMI.

- (Somente políticas de ciclo de vida de snapshot) Se mais de um dos agendamentos iniciados estiver habilitado para restauração rápida de snapshots, o snapshot será habilitado para restauração rápida de snapshots em todas as zonas de disponibilidade especificadas em todos os agendamentos iniciados. As configurações de retenção mais altas dos agendamentos iniciados são usadas para cada zona de disponibilidade.

- Se mais de um dos agendamentos iniciados estiver habilitado para cópia entre regiões, o snapshot ou a AMI serão copiados para todas as regiões especificadas em todos os agendamentos iniciados. O período de retenção mais alta dos agendamentos iniciados é aplicado.

Tags do recurso-alvo (somente políticas personalizadas)

As políticas personalizadas do Amazon Data Lifecycle usam tags de recurso para identificar os recursos para backup. Ao criar um snapshot ou uma política de AMI baseada no EBS, você pode especificar várias tags de recursos de destino. Todos os recursos do tipo especificado (instância ou volume) que tenham pelo menos uma das tags de recursos de destino especificadas serão visados pela política. Por exemplo, se você criar uma política de snapshot direcionada a volumes e especificar `purpose=prod`, `costcenter=prod`, e `environment=live` como tags de recurso de destino, a política visará todos os volumes que tenham qualquer um desses pares de valores de chave de tag.

Se você quiser executar várias políticas em um recurso, poderá atribuir várias tags ao recurso de destino e, em seguida, criar políticas separadas para cada uma direcionar uma tag de recurso específica.

Não é possível usar os caracteres \ ou = em uma chave de etiquetas. Tags de recursos de destino diferenciam letras maiúsculas de minúsculas. Para obter mais informações, consulte Marcar seus recursos.

Snapshots

Os snapshots são o principal meio de fazer backup de dados de volumes do EBS. Para economizar custos de armazenamento, os snapshots sucessivos são incrementais, contendo apenas os dados do volume que mudaram desde o snapshot anterior. Quando você exclui um snapshot de uma série de snapshots de um volume, somente os dados exclusivos daquele snapshot são removidos. Os dados restantes do histórico capturado do volume são preservados. Para ter mais informações, consulte Snapshots do Amazon EBS.

AMIs apoiadas pelo EBS

Uma Imagem de máquina da Amazon (AMI) fornece as informações necessárias para iniciar uma instância. É possível executar várias instâncias em uma única AMI quando precisa de várias instâncias com a mesma configuração. O Amazon Data Lifecycle Manager é compatível apenas com AMIs com EBS. AMIs apoiadas pelo EBS incluem um snapshot para cada volume do EBS associado

à instância de origem. Para obter mais informações, consulte Imagens de máquina da Amazon (AMIs).

Tags do Amazon Data Lifecycle Manager

O Amazon Data Lifecycle Manager aplica as seguintes tags do sistema a todos os snapshots e AMIs criados por uma política a fim de distingui-los dos snapshots e AMIs criados por outros meios:

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`
- `aws:dlm:expirationTime`: para snapshots criados por uma programação baseada em idade. Indica quando o snapshot deve ser excluído do nível padrão.
- `dlm:managed`
- `aws:dlm:archived`: para snapshots que foram arquivados de acordo com uma programação.
- `aws:dlm:pre-script`: para snapshots criados com scripts prévios.
- `aws:dlm:post-script`: para snapshots criados com scripts posteriores.

Também é possível especificar tags personalizadas para aplicar durante a criação de um snapshot e AMIs. Não é possível usar os caracteres \ ou = em uma chave de etiquetas.

As tags de destino que o Amazon Data Lifecycle Manager usa para associar os volumes à política podem ser aplicadas opcionalmente aos snapshots criados pela política. Da mesma forma, as tags de destino usadas para associar instâncias a uma política de AMI podem, opcionalmente, ser aplicadas às AMIs criadas pela política.

Comparação entre políticas padrão e políticas personalizadas

Esta seção compara as políticas padrão e as políticas personalizadas, e destaca suas semelhanças e diferenças.

Tópicos

- Comparação de políticas de snapshots do EBS
- Comparação das políticas de AMI baseadas no EBS

Comparação de políticas de snapshots do EBS

A tabela a seguir destaca as diferenças entre a política padrão para snapshots do EBS e as políticas personalizadas de snapshot do EBS.

Atributo	Política padrão para snapshots do EBS	Política personalizada de snapshots do EBS
Recurso de backup gerenciado	Snapshot do EBS	Snapshot do EBS
Tipos de recursos-alvo	Volumes	Volumes ou instâncias
Seleção de recursos-alvo	Tem como alvo todos os volumes da região que não têm snapshots recentes. Você pode especificar parâmetros de exclusão para excluir volumes específicos.	Tem como alvo somente os volumes ou as instâncias que têm tags específicas.
Parâmetros de exclusão	Sim, pode excluir volumes de inicializ ação, tipos de volume específicos e volumes com tags específicas.	Sim, pode excluir volumes de inicializ ação e volumes com tags específicas quando tem como alvo as instâncias.
Support AWS Outposts	Não	Sim
Compatibilidade com várias agendas	Não	Sim, até quatro agendas por política
Tipos de retenção compatíveis	Retenção baseada em tempo apenas	Retenção com base em tempo e quantidade
Frequência de criação de snapshots	A cada 1 a 7 dias.	Frequência diária, semanal, mensal, anual ou personalizada usando uma expressão cron.

Atributo	Política padrão para snapshots do EBS	Política personalizada de snapshots do EBS
Retenção de snapshots	2 a 14 dias.	Até 1.000 snapshots (baseado em quantidade) ou até 100 anos (baseado em tempo).
Compatibilidade com snapshots consistentes com a aplicação	Não	Sim, usando scripts prévios e posteriores
Compatibilidade com arquivamento de snapshots	Não	Sim
Compatibilidade com restauração rápida de snapshots	Não	Sim
Compatibilidade com cópia entre regiões	Sim, com as configurações padrão [1]	Sim, com configurações personalizadas
Compatibilidade com compartilhamento entre contas	Não	Sim
Compatibilidade com exclusão estendida [2]	Sim	Não

[1] Para políticas padrão:

- Você não pode copiar tags em cópias entre regiões.
- As cópias usam o mesmo período de retenção que o snapshot original.

- Os snapshots recebem o mesmo status de criptografia que o volume original. Se a região de destino estiver habilitada para criptografia por padrão, as cópias sempre serão criptografadas, mesmo que os snapshots originais estejam descriptografados. As cópias são sempre criptografadas com a chave do KMS padrão para a região de destino.

[2] Para políticas padrão e personalizadas:

- Se uma instância ou volume-alvo for excluído, o Amazon Data Lifecycle Manager continuará excluindo snapshots até restar apenas o último com base no período de retenção. Para as políticas padrão, você pode estender a exclusão para incluir o último snapshot.
- Se uma política for excluída ou entrar em estado de erro ou de desabilitada, o Amazon Data Lifecycle Manager interromperá a exclusão dos snapshots. Para as políticas padrão, você pode estender a exclusão para continuar a excluir os snapshots, inclusive o último.

Comparação das políticas de AMI baseadas no EBS

A tabela a seguir destaca as diferenças entre a política padrão para AMIs baseadas no EBS e as políticas personalizadas de AMI baseada no EBS.

Atributo	Política padrão para AMIs baseadas no EBS	Política personalizada de AMI baseada no EBS
Recurso de backup gerenciado	AMIs apoiadas pelo EBS	AMIs apoiadas pelo EBS
Tipos de recursos-alvo	Instâncias	Instâncias
Seleção de recursos-alvo	Tem como alvo todas as instância s na região que não têm AMIs recentes. Você pode especificar parâmetros de exclusão para excluir instâncias específicas.	Tem como alvo somente as instância s que têm tags específicas.
Reinicializar instâncias antes	Não	Sim

Atributo	Política padrão para AMIs baseadas no EBS	Política personalizada de AMI baseada no EBS
da criação da AMI		
Parâmetros de exclusão	Sim, pode excluir instâncias com tags específicas.	Não
Compatibilidade com várias agendas	Não	Sim, até quatro agendas por política.
Frequência de criação de AMI	A cada 1 a 7 dias.	Frequência diária, semanal, mensal, anual ou personalizada usando uma expressão cron.
Tipos de retenção compatíveis	Retenção baseada em tempo apenas.	Retenção baseada em tempo e quantidade.
Retenção de AMIs	2 a 14 dias.	Até 1.000 AMIs (baseada em quantidade) ou até 100 anos (baseada em tempo).
Compatibilidade com descontinuação de AMIs	Não	Sim
Compatibilidade com cópia entre regiões	Sim, com as configurações padrão [1]	Sim, com configurações personalizadas
Compatibilidade com exclusão estendida [2]	Sim	Não

[1] Para políticas padrão:

- Você não pode copiar tags em cópias entre regiões.
- As cópias usam o mesmo período de retenção que a AMI original.
- Os snapshots recebem o mesmo status de criptografia que a AMI original. Se a região de destino estiver habilitada para criptografia por padrão, as cópias sempre serão criptografadas, mesmo que as AMIs originais estejam descriptografados. As cópias são sempre criptografadas com a chave do KMS padrão para a região de destino.

[2] Para políticas padrão e personalizadas:

- Se uma instância-alvo for encerrada, o Amazon Data Lifecycle Manager continuará excluindo AMIs até restar apenas a última com base no período de retenção. Para políticas padrão, você pode estender o cancelamento de registro para incluir a última AMI.
- Se uma política for excluída ou entrar em estado de erro ou de desabilitada, o Amazon Data Lifecycle Manager interromperá a exclusão das AMIs. Para as políticas padrão, você pode estender a exclusão para continuar a cancelar o registro das AMIs, inclusive da última.

Políticas padrão

Para criar AMIs periódicas baseadas no EBS das instâncias, use a política padrão para AMIs baseadas no EBS. Para criar snapshots de todos os volumes, qualquer que seja seu estado de anexação, ou se você quiser excluir volumes específicos, use a política padrão para snapshots do EBS.

Esta seção explica como criar políticas padrão.

Tópicos

Considerações

Ao trabalhar com políticas padrão, tenha em mente o seguinte:

- As políticas padrão não fazem backup dos recursos-alvo (instâncias ou volumes) que têm backups recentes (snapshots ou AMIs). A frequência de criação determina de quais recursos são feitos backups. O backup de um volume ou instância é feito somente se seu último snapshot ou AMI for mais antigo que a frequência de criação da política. Por exemplo, se você especificar uma frequência de criação de três dias, a política padrão para snapshots do EBS só criará um snapshot de um volume se o último snapshot tiver sido feito há mais de 3 dias.
- Por padrão, as políticas padrão têm como alvo todas as instâncias ou volumes na região, a menos que parâmetros de exclusão sejam especificados.
- As políticas padrão criarão um conjunto mínimo de snapshots exclusivos. Por exemplo, se você habilitar a política de AMI baseada no EBS e a política de snapshot do EBS, a política de snapshot não duplicará os snapshots dos volumes que já foram copiados para backup pela política de AMI baseada no EBS.
- As políticas padrão só começarão a ter como alvo os recursos criados há pelo menos 24 horas.
- Se você excluir um volume ou encerrar uma instância que seja alvo de uma política padrão, o Amazon Data Lifecycle Manager continuará a excluir os backups criados anteriormente (snapshots ou AMIs) de acordo com o período de retenção até restar apenas um backup. Você deve excluir esse backup manualmente se ele não for necessário.

  Se você quiser que o Amazon Data Lifecycle Manager exclua o último backup, você poderá habilitar a exclusão estendida.
- Se uma política for excluída ou entrar em estado de erro ou de desabilitada, o Amazon Data Lifecycle Manager interromperá a exclusão dos backups criados anteriormente (snapshots ou AMIs). Se você quiser que o Amazon Data Lifecycle Manager continue excluindo os backups, inclusive o último, deverá habilitar a exclusão estendida antes de excluir a política ou antes que o estado da política mude para desabilitada ou excluída.
- Quando você cria e habilita uma política padrão, o Amazon Data Lifecycle Manager atribui aleatoriamente aos recursos-alvo uma janela de quatro horas. Os recursos-alvo são copiados durante a janela que foi atribuída a eles na frequência de criação especificada. Por exemplo, se uma política tiver uma frequência de criação de 3 dias e se a um recurso-alvo for atribuída a janela das 12h às 16h, o backup desse recurso será feito entre 12h e 16h a cada 3 dias.

Política padrão para snapshots do EBS

O procedimento a seguir mostra como criar uma política padrão para snapshots do EBS.

Console

Para criar uma política padrão para snapshots do EBS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Lifecycle Manager e depois Criar política de ciclo de vida.
3. Para Tipo de política, escolha Política padrão e depois Política de snapshot do EBS.
4. Para Description (Descrição), insira uma breve descrição da rota.
5. Para Perfil do IAM, escolha o perfil do IAM que tem permissões para gerenciar snapshots.

   Recomendamos que você escolha Padrão para usar o perfil do IAM padrão fornecido pelo Amazon Data Lifecycle Manager. Porém, também é possível usar um perfil do IAM personalizado que você criou anteriormente.
6. Em Frequência de criação, especifique com que frequência você deseja que a política seja executada e crie snapshots dos seus volumes.

   A frequência especificada também determina de quais volumes será feito backup. A política só fará backup dos volumes cujo backup não foi feito por nenhum outro meio dentro da frequência especificada. Por exemplo, se você especificar uma frequência de criação de três dias, a política só criará snapshots dos volumes cujo backup não foi feito nos últimos três dias.
7. Para Período de retenção, especifique por quanto tempo você deseja que a política retenha os snapshots que ela criar. Quando um snapshot atinge o limite de retenção, ele é automaticamente excluído. O período de retenção deve ser maior ou igual ao intervalo de criação.
8. (Opcional) Configure os parâmetros de exclusão para excluir volumes específicos dos backups agendados. Os volumes excluídos não serão copiados quando a política for executada.

   a. Para excluir os volumes de inicialização, selecione Excluir volumes de inicialização. Se você excluir os volumes de inicialização, somente os volumes de dados (não de inicialização) serão copiados pela política. Em outras palavras, ela não criará snapshots de volumes anexados às instâncias como volumes de inicialização.

   b. Para excluir tipos de volume específicos, escolha Excluir tipos de volume específicos e selecione os tipos de volume a serem excluídos. A política só fará backup de volumes de outros tipos.

c. Para excluir volumes que têm tags específicas, escolha Adicionar tag e depois especifique as chaves e os valores de tag. A política não criará snapshots de volumes que contêm alguma das tags especificadas.

9. (Opcional) Para Configurações avançadas, especifique as ações adicionais que a política deve realizar.

   a. (Opcional) Para copiar automaticamente as tags atribuídas do volume original para os snapshots, selecione Copiar tags dos volumes.

   b. Com a exclusão estendida desabilitada:

      - Se o volume original for excluído, o Amazon Data Lifecycle Manager continuará excluindo snapshots criados anteriormente até restar apenas o último com base no período de retenção. Se você quiser que o Amazon Data Lifecycle Manager exclua todos os snapshots, inclusive o último, selecione Estender exclusão.
      - Se uma política for excluída ou entrar em estado de `error`ou de `disabled`, o Amazon Data Lifecycle Manager interromperá a exclusão dos snapshots. Se você quiser que o Amazon Data Lifecycle Manager continue a excluir os snapshots, inclusive o último, selecione Estender exclusão.

      > **Note**
      >
      > Se você habilitar a exclusão estendida, substituirá ambos os comportamentos descritos acima simultaneamente.

   c. Para copiar os snapshots criados pela política para outras regiões, selecione Criar cópia entre regiões e depois selecione até três regiões de destino.

      - Se o snapshot original estiver criptografado ou se a criptografia estiver habilitada por padrão para a região de destino, os snapshots copiados serão criptografados usando a chave do KMS padrão para criptografia do EBS na região de destino.
      - Se o snapshot original não estiver criptografado e a criptografia estiver desabilitada por padrão para a região de destino, os snapshots copiados serão descriptografados.

10. (Opcional) Para adicionar uma tag à política, escolha Adicionar tag e especifique o par chave-valor da tag.

11. Escolha Criar política padrão.

> **Note**
>
> Se receber um erro `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consulte Solução de problemas para obter mais informações.

AWS CLI

Para criar uma política padrão para snapshots do EBS

Use o comando create-lifecycle-policy. Você pode especificar os parâmetros de solicitação com um de dois métodos, dependendo do seu caso de uso ou de suas preferências:

- Método 1

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeBootVolumes=true | false,
 ExcludeTags=[{Key=tag_key,Value=tag_value}], ExcludeVolumeTypes="standard | gp2 |
 gp3 | io1 | io2 | st1 | sc1"
```

Por exemplo, para criar uma política padrão para snapshots do EBS que tenha como alvo todos os volumes na região, use o perfil do IAM padrão, seja executada diariamente (padrão) e retenha snapshots por 7 dias (padrão), você precisa especificar os seguintes parâmetros:

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default snapshot policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRole \
--default-policy VOLUME
```

- Método 2

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--policy-details file://policyDetails.json
```

Em que `policyDetails.json` inclui o seguinte:

```
{
    "PolicyLanguage": "SIMPLIFIED",
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceType": "VOLUME",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
    "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeBootVolume": true | false,
  "ExcludeVolumeTypes": ["standard | gp2 | gp3 | io1 | io2 | st1 | sc1"],
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

Política padrão para AMIs baseadas no EBS

O procedimento a seguir mostra como criar uma política padrão para AMIs baseadas no EBS.

Console

Para criar uma política padrão para AMIs baseadas no EBS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Lifecycle Manager e depois Criar política de ciclo de vida.

3. Para Tipo de política, escolha Política padrão e depois Política de AMI baseada no EBS.
4. Para Description (Descrição), insira uma breve descrição da rota.
5. Para Perfil do IAM, escolha o perfil do IAM que tem permissões para gerenciar AMIs.

   Recomendamos que você escolha Padrão para usar o perfil do IAM padrão fornecido pelo Amazon Data Lifecycle Manager. Porém, também é possível usar um perfil do IAM personalizado que você criou anteriormente.
6. Para Frequência de criação, especifique com que frequência você deseja que a política seja executada e crie snapshots das instâncias.

   A frequência especificada também determina de quais instâncias será feito backup. A política só fará backup das instâncias cujo backup não foi feito por nenhum outro meio dentro da frequência especificada. Por exemplo, se você especificar uma frequência de criação de três dias, a política só criará AMIs das instâncias cujo backup não foi feito nos últimos três dias.
7. Para Período de retenção, especifique por quanto tempo você deseja que a política retenha as AMIs que ela criar. Quando uma AMI atinge o limite de retenção, seu registro é automaticamente cancelado e os snapshots a ela associados são excluídos. O período de retenção deve ser maior ou igual ao intervalo de criação.
8. (Opcional) Configure os Parâmetros de exclusão para excluir instâncias específicas dos backups agendados. O backup das instâncias excluídas não será feito quando a política for executada.

   - Para excluir volumes que tenham tags específicas, escolha Adicionar tag e depois especifique as chaves e os valores da tag. A política não criará AMIs de instâncias que tenham alguma das tags especificadas.
9. (Opcional) Para Configurações avançadas, especifique as ações adicionais que a política deve realizar.

   a. Para copiar as tags atribuídas das instâncias originais para suas AMIs, selecione Copiar tags das instâncias.

   b. Com a exclusão estendida desabilitada:

      - Se uma instância original for encerrada, o Amazon Data Lifecycle Manager continuará a cancelar os registros das AMIs até restar apenas a última com base no período de retenção. Se você quiser que o Amazon Data Lifecycle Manager cancele o registro de todas as AMIs, inclusive da última, selecione Estender exclusão.

- Se uma política for excluída ou entrar no estado de `error` ou de `disabled`, o Amazon Data Lifecycle Manager interromperá o cancelamento do registro das AMIs. Se você quiser que o Amazon Data Lifecycle Manager continue a cancelar o registo de todas as AMIs, inclusive da última, selecione Estender exclusão.

> **Note**
>
> Se você habilitar a exclusão estendida, substituirá ambos os comportamentos descritos acima simultaneamente.

c. Para copiar as AMIs criadas pela política para outras regiões, selecione Criar cópia entre regiões e depois selecione até três regiões de destino.

- Se a AMI original estiver criptografada ou se a criptografia estiver habilitada por padrão para a região de destino, as AMIs copiadas serão criptografadas usando a chave do KMS padrão para criptografia do EBS na região de destino.
- Se a AMI original não estiver criptografada e a criptografia estiver desabilitada por padrão para a região de destino, as AMIs copiadas serão descriptografadas.

10. (Opcional) Para adicionar uma tag à política, escolha Adicionar tag e especifique o par chave-valor da tag.
11. Escolha Criar política padrão.

> **Note**
>
> Se receber um erro `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists`, consulte Solução de problemas para obter mais informações.

AWS CLI

Para criar uma política padrão para AMIs baseadas no EBS

Use o comando create-lifecycle-policy. Você pode especificar os parâmetros de solicitação com um de dois métodos, dependendo do seu caso de uso ou de suas preferências:

- Método 1

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeTags=[{Key=tag_key,Value=tag_value}]
```

Por exemplo, para criar uma política padrão para AMIs baseadas no EBS que tenha como alvo todas as instâncias na região, use o perfil do IAM padrão, seja executada diariamente (padrão) e retenha AMIs por 7 dias (padrão), você precisa especificar os seguintes parâmetros:

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default AMI policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement \
--default-policy INSTANCE
```

- Método 2

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--policy-details file://policyDetails.json
```

Em que `policyDetails.json` inclui o seguinte:

```
{
    "PolicyLanguage": "SIMPLIFIED",
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceType": "INSTANCE",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
```

```
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
 "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

Habilite políticas padrão em todas as contas e regiões

Usando AWS CloudFormation StackSets, você pode habilitar as políticas padrão do Amazon Data Lifecycle Manager em várias contas e AWS regiões com uma única operação.

Você pode usar conjuntos de pilhas para habilitar políticas padrão de uma das seguintes formas:

- Em toda a AWS organização — garante que as políticas padrão sejam habilitadas e configuradas de forma consistente em toda a AWS organização ou em unidades organizacionais específicas de uma organização. Isso é feito usando permissões gerenciadas pelo serviço. AWS CloudFormation StackSets cria as funções necessárias do IAM em seu nome.
- Em AWS contas específicas — Garante que as políticas padrão sejam ativadas e configuradas de forma consistente em contas específicas de destino. Isso requer permissões autogerenciadas. Você cria as funções do IAM necessárias para estabelecer a relação de confiança entre a conta do administrador do conjunto de pilhas e as contas de destino.

Para obter mais informações, consulte Modelos de permissão para conjuntos de pilhas no Guia do AWS CloudFormation usuário.

Use os procedimentos a seguir para habilitar as políticas padrão do Amazon Data Lifecycle Manager em toda a AWS organização, em OUs específicas ou em contas de destino específicas.

Pré-requisitos

Siga um destes procedimentos, dependendo de como você está habilitando as políticas padrão:

- (Em todas AWS as organizações) Você deve habilitar todos os recursos em sua organização e ativar o acesso confiável com AWS Organizations. Você também deve usar a conta de gerenciamento da organização ou uma conta de administrador delegado.
- (Em contas de destino específicas) Você deve conceder permissões autogerenciadas criando as funções necessárias para estabelecer uma relação confiável entre a conta de administrador do conjunto de pilhas e as contas de destino.

Console

Para habilitar políticas padrão em uma AWS organização ou em contas específicas

1. Abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.
2. No painel de navegação, escolha e, em seguida StackSets, escolha Criar StackSet.
3. Em Permissões, faça o seguinte, dependendo de como você está habilitando as políticas padrão:
   - (Em toda a AWS organização) Escolha as permissões gerenciadas pelo serviço.
   - (Em contas específicas) Escolha permissões de autoatendimento. Em seguida, para a função de administrador do IAM ARN, selecione a função de serviço do IAM que você criou para a conta do administrador e, para o nome da função de execução do IAM, insira o nome da função de serviço do IAM que você criou nas contas de destino.
4. Em Preparar modelo, escolha Usar um modelo de amostra.
5. Para modelos de amostra, faça o seguinte:
   - (Política padrão para snapshots do EBS) Selecione Criar políticas padrão do Amazon Data Lifecycle Manager para snapshots do EBS.
   - (Política padrão para AMIs suportadas pelo EBS) Selecione Criar políticas padrão do Amazon Data Lifecycle Manager para AMIs suportadas pelo EBS.
6. Selecione Next (Próximo).
7. Para StackSet nome e StackSet descrição, insira um nome descritivo e uma breve descrição.
8. Na seção Parâmetros, defina as configurações de política padrão conforme necessário.

> **Note**
>
> Para cargas de trabalho críticas, recomendamos CreateInterval = 1 dia e RetainInterval = 7 dias.

9. Selecione Next (Próximo).
10. (Opcional) Para Tags, especifique tags para ajudá-lo a identificar StackSet e empilhar recursos.
11. Em Execução gerenciada, escolha Ativo.
12. Selecione Next (Próximo).
13. Em Add stacks to stack set (Adicionar pilhas ao conjunto de pilhas), escolha Deploy new stacks (Implantar novas pilhas).
14. Siga um destes procedimentos, dependendo de como você está habilitando as políticas padrão:
    - (Em toda a AWS organização) Para destinos de implantação, escolha uma das seguintes opções:
      - Para implantar em toda a AWS organização, escolha Implantar na organização.
      - Para implantar em unidades organizacionais (OU) específicas, escolha Implantar em unidades organizacionais e, em seguida, para ID da OU, insira a ID da OU. Para adicionar OUs adicionais, escolha Adicionar outra OU.
    - (Em contas de destino específicas) Em Contas, faça o seguinte:
      - Para implantar em contas de destino específicas, escolha Implantar pilhas em contas e, em Números de conta, insira as IDs das contas de destino.
      - Para implantar em todas as contas em uma OU específica, escolha Implantar pilha em todas as contas em uma unidade organizacional e, em seguida, em Números da organização, insira a ID da OU de destino.
15. Em Implantação automática, escolha Ativado.
16. Em Comportamento de remoção de conta, escolha Retain stacks.
17. Em Especificar regiões, selecione regiões específicas nas quais ativar as políticas padrão ou escolha Adicionar todas as regiões para ativar as políticas padrão em todas as regiões.
18. Selecione Next (Próximo).

19. Analise as configurações do conjunto de pilhas, selecione Eu reconheço que AWS CloudFormation pode criar recursos do IAM e, em seguida, escolha Enviar.

AWS CLI

Para habilitar políticas padrão em uma AWS organização

1. Crie o conjunto de pilhas. Use o comando create-stack-set.

   Em `--permission-model`, especifique `SERVICE_MANAGED`.

   Para`--template-url`, especifique um dos seguintes URLs de modelo:

   - (Políticas padrão para AMIs apoiadas pelo EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`
   - (Políticas padrão para snapshots do EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml`

   Para`--parameters`, especifique as configurações das políticas padrão. Para obter parâmetros compatíveis, descrições de parâmetros e valores válidos, baixe o modelo usando a URL e, em seguida, visualize o modelo usando um editor de texto.

   Em `--auto-deployment`, especifique `Enabled=true, RetainStacksOnAccountRemoval=true`.

   ```
   $ aws cloudformation create-stack-set \
   --stack-set-name stackset_name \
   --permission-model SERVICE_MANAGED \
   --template-url template_url \
   --parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
    "ParameterKey=param_name_2,ParameterValue=param_value_2" \
   --auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
   ```

2. Implante o conjunto de pilhas. Use o comando create-stack-instances.

   Para`--stack-set-name`, especifique o nome do conjunto de pilhas que você criou na etapa anterior.

Para `--deployment-targets OrganizationalUnitIds`, especifique a ID da OU raiz a ser implantada em toda a organização ou IDs da OU a ser implantada em OUs específicas na organização.

Para `--regions`, especifique as AWS regiões nas quais habilitar as políticas padrão.

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--deployment-targets OrganizationalUnitIds='["root_ou_id"]' | '["ou_id_1",
 "ou_id_2]' \
--regions '["region_1", "region_2"]'
```

Para habilitar políticas padrão em contas de destino específicas

1. Crie o conjunto de pilhas. Use o comando create-stack-set.

   Para `--template-url`, especifique um dos seguintes URLs de modelo:

   - (Políticas padrão para AMIs apoiadas pelo EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`
   - (Políticas padrão para snapshots do EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml`

   Para `--administration-role-arn`, especifique o ARN da função de serviço do IAM que você criou anteriormente para o administrador do conjunto de pilhas.

   Para `--execution-role-name`, especifique o nome da função de serviço do IAM que você criou nas contas de destino.

   Para `--parameters`, especifique as configurações das políticas padrão. Para obter parâmetros compatíveis, descrições de parâmetros e valores válidos, baixe o modelo usando a URL e, em seguida, visualize o modelo usando um editor de texto.

   Em `--auto-deployment`, especifique `Enabled=true,RetainStacksOnAccountRemoval=true`.

```
$ aws cloudformation create-stack-set \
--stack-set-name stackset_name \
--template-url template_url \
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
 "ParameterKey=param_name_2,ParameterValue=param_value_2" \
--administration-role-arn administrator_role_arn \
--execution-role-name target_account_role \
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. Implante o conjunto de pilhas. Use o comando create-stack-instances.

   Para `--stack-set-name`, especifique o nome do conjunto de pilhas que você criou na etapa anterior.

   Para `--accounts`, especifique os IDs das AWS contas de destino.

   Para `--regions`, especifique as AWS regiões nas quais habilitar as políticas padrão.

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--accounts '["account_ID_1","account_ID_2"]' \
--regions '["region_1", "region_2"]'
```

Políticas personalizadas

Esta seção explica como criar políticas personalizadas de snapshot do EBS, de AMI baseada no EBS e de eventos de cópia entre contas.

Tópicos

- Automação dos ciclos de vida do snapshot
- Automatizar ciclos de vida da AMI
- Automatizar cópias de snapshots entre contas

Automação dos ciclos de vida do snapshot

O procedimento a seguir mostra como usar o Amazon Data Lifecycle Manager para automatizar os ciclos de vida de snapshots do Amazon EBS.

Tópicos

Criar uma política de ciclo de vida de snapshots

Use um dos procedimentos a seguir para criar uma política de ciclo de vida de snapshots.

Console

Para criar uma política de snapshot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Na tela Select policy type (Selecionar tipo de política), escolha EBS snapshot policy (Política de snapshot do EBS) e depois Next (Próximo).
4. Na seção Target resources (Recursos de destino), faça o seguinte:
   a. Em Target resource types, (Tipos de recurso de destino), escolha o tipo de recurso para backup. Escolha `Volume` (Volume) para criar snapshots de volumes individuais ou `Instance` (Instância) para criar snapshots multivolume dos volumes associados a uma instância.
   b. (Somente para clientes do AWS Outpost) Especifique onde os recursos de destino estão localizados.

      Para Local dos recursos-alvo, especifique onde os recursos-alvo estão localizados.

- Se os recursos de destino estiverem localizados em uma AWS região, escolha AWS Região. O Amazon Data Lifecycle Manager faz backup de todos os recursos do tipo especificado que têm etiquetas de destino correspondentes somente na região atual. Se o recurso estiver localizado em uma região, os snapshots criados pela política serão armazenados na mesma região.
- Se os recursos de destino estiverem localizados em um Outpost em sua conta, escolha AWS Outpost. O Amazon Data Lifecycle Manager faz backup de todos os recursos do tipo especificado que tenham etiquetas de destino correspondentes em todos os Outposts em sua conta. Se o recurso estiver localizado em um Outpost, os snapshots criados pela política poderão ser armazenados na mesma região ou no mesmo Outpost que o recurso.
- Se você não tiver nenhum Outposts em sua conta, essa opção ficará oculta e a AWS Região será selecionada para você.

c. Em Target with these tags (Destino com essas etiquetas), escolha as etiquetas de recurso que identificam os volumes ou as instâncias dos quais fazer backup. A política só oferece suporte aos recursos com a chave de tag e os pares de valor especificados.

5. Para Description (Descrição), insira uma breve descrição da rota.
6. Em IAM role (Função do IAM), selecione a função do IAM que tem permissões para gerenciar snapshots e para descrever volumes e instâncias. Para usar a função padrão fornecida pelo Amazon Data Lifecycle Manager, escolha Default role (Função padrão). Se preferir, para usar uma função do IAM personalizada criada anteriormente, selecione Choose another role (Escolher outra função) e selecione a função a ser usada.
7. Em Policy tags (Etiquetas de políticas), adicione as etiquetas a serem aplicadas na política de ciclo de vida. É possível usar essas etiquetas para identificar e categorizar suas políticas.
8. Em Policy status (Status da política), selecione Enable (Habilitar) para iniciar as execuções da política no próximo horário agendado ou Disable policy (Desabilitar política) para impedir que a política seja executada. Se você não habilitar a política agora, ela não começará a criar snapshots até que você a ative manualmente após a criação.
9. (Políticas que têm apenas instâncias como alvo) Excluir volumes de conjuntos de snapshots de vários volumes.

   Por padrão, o Amazon Data Lifecycle Manager criará snapshots de todos os volumes anexados às instâncias-alvo. Porém, você pode optar por criar snapshots de um subconjunto dos volumes anexados. Na seção Parameters (Parâmetros), faça o seguinte:

- Se não quiser criar snapshots dos volumes raiz anexados às instâncias de destino, selecione Exclude root volume (Excluir volume raiz). Se você selecionar essa opção, apenas os volumes de dados (não raiz) anexados às instâncias de destino serão incluídos nos conjuntos de snapshots de vários volumes.
- Para criar snapshots de um subconjunto dos volumes de dados (não raiz) anexados às instâncias de destino, selecione Exclude specific data volumes (Excluir volumes de dados específicos) e especifique as etiquetas a serem usadas para identificar os volumes de dados que não deverão ser capturados. O Amazon Data Lifecycle Manager não criará snapshots de volumes de dados que contenham qualquer uma das etiquetas especificadas. O Amazon Data Lifecycle Manager criará snapshots apenas de volumes de dados que não contenham qualquer uma das etiquetas especificadas.

10. Selecione Next (Próximo).
11. Em Configure schedule (Configurar agendamento), configure os agendamentos de política. Uma política pode ter até quatro agendamentos. A Programação 1 é obrigatória. As Programações 2, 3 e 4 são opcionais. Para cada agendamento de política que você adicionar, faça o seguinte:

    a. Na seção Schedule details (Detalhes do agendamento), faça o seguinte:

        i. Em Schedule name (Nome do agendamento), especifique um nome descritivo para o agendamento.

        ii. Em Frequency (Frequência) e nos campos relacionados, configure o intervalo entre as execuções da política.

        É possível configurar execuções de políticas com uma programação diária, semanal, mensal ou anual. Como opção, escolha Custom cron expression (Expressão cron personalizada) para especificar um intervalo de até 1 ano. Para obter mais informações, consulte Expressões Cron no Guia do usuário do Amazon CloudWatch Events.

        > **Note**
        >
        > Se precisar habilitar o arquivamento de snapshots para a programação, você deve selecionar a frequência mensal ou anual, ou especificar uma expressão cron com uma frequência de criação de pelo menos 28 dias.

Se você especificar uma frequência mensal que crie snashots em um dia específico de uma semana específica (por exemplo, na segunda quinta-feira do mês), para uma programação baseada em contagem, a contagem de retenção para o nível de arquivamento deverá ser 4 ou mais.

iii. Em Starting at (Iniciando às), especifique a hora em que as execuções da política estão programadas para iniciar. A primeira execução da política começa uma hora depois do horário agendado. A hora deve ser inserida no formato `hh:mm` UTC.

iv. Em Retention type (Tipo de retenção), especifique a política de retenção para snapshots criados pelo agendamento.

É possível reter snapshots com base na contagem total ou na idade deles.

- Retenção baseada em contagem
  - Com o arquivamento de snapshots desabilitado, o intervalo varia de `1` a `1000`. Quando o limite de retenção for atingido, o snapshot mais antigo será excluído permanentemente.
  - Com o arquivamento de snapshots habilitado, o intervalo varia de `0` (arquivamento imediatamente após a criação) a `1000`. Quando o limite de retenção for atingido, o snapshot mais antigo será convertido em um snapshot completo e movido para o nível de arquivamento.
- Retenção com base em tempo
  - Com o arquivamento de snapshots desabilitado, o intervalo varia de `1` dia a `100` anos. Quando o limite de retenção for atingido, o snapshot mais antigo será excluído permanentemente.
  - Com o arquivamento de snapshots habilitado, o intervalo varia de `0` dias (arquivamento imediatamente após a criação) a `100` anos. Quando o limite de retenção for atingido, o snapshot mais antigo será convertido em um snapshot completo e movido para o nível de arquivamento.

Note

- Todas as programações devem ter o mesmo tipo de retenção (baseado em idade ou contagem). É possível especificar o tipo de retenção somente para a Programação 1. As Programações 2, 3 e 4 herdam o tipo

de retenção da Programação 1. Cada programação pode ter sua própria contagem ou período de retenção.

- Se você habilitar a restauração rápida de snapshots, a cópia entre regiões ou o compartilhamento de snapshots, deverá especificar uma contagem de retenção de 1 ou mais, ou um período de retenção de 1 dia ou mais.

v. (somente para AWS Outposts clientes) Especifique o destino do snapshot.

Para Destino do snapshot, especifique o destino dos snapshots criados pela política.

- Se a política tem como alvo recursos em uma região, os instantâneos devem ser criados na mesma região. AWS A região está selecionada para você.
- Se a política se destina aos recursos de um Outpost, é possível escolher criar os snapshots no mesmo Outpost que o recurso de origem ou na região que está associada ao Outpost.
- Se você não tiver nenhum Outposts em sua conta, essa opção ficará oculta e a AWS Região será selecionada para você.

b. Configure a marcação para snapshots.

Na seção Tagging (Marcação), faça o seguinte:

i. Para copiar todas as etiquetas definidas por usuário do volume de origem para os snapshots criados pelo agendamento, selecione Copy tags from source (Copiar etiquetas da origem).

ii. Para especificar etiquetas adicionais a serem atribuídas aos snapshots criados por esse agendamento, escolha Add tags (Adicionar etiquetas).

c. Configurar scripts prévios e posteriores para snapshots consistentes com a aplicação.

Para ter mais informações, consulte Automatizar snapshots consistentes com a aplicação com scripts prévios e posteriores.

d. (Políticas que têm somente volumes como alvo) Configurar o arquivamento dos snapshots.

Na seção Arquivamento de snapshots, faça o seguinte:

> **Note**
>
> Você só pode habilitar o arquivamento de snapshots para uma única programação em uma política.

i. Para habilitar o arquivamento de snapshots para a programação, selecione Archive snapshots created by this schedule (Arquivar os snapshots criados por essa programação).

> **Note**
>
> Você só pode habilitar o arquivamento de snapshots se a frequência de criação de snapshots for mensal ou anual, ou se especificar uma expressão cron com uma frequência de criação de pelo menos 28 dias.

ii. Especifique a regra de retenção para snapshots no nível de arquivamento.

- Para programações baseadas em contagem, especifique o número de snapshots a serem retidos no nível de arquivamento. Quando o limite de retenção for atingido, o snapshot mais antigo será excluído permanentemente do nível de arquivamento. Por exemplo, se você especificar 3, a programação reterá no máximo 3 snapshots no nível de arquivamento. Quando o quarto snapshot for arquivado, o mais antigo dos três snapshots existentes no nível de arquivamento será excluído.
- Para programações baseadas em idade, especifique por quanto tempo os snapshots devem ser retidos no nível de arquivamento. Quando o limite de retenção for atingido, o snapshot mais antigo será excluído permanentemente do nível de arquivamento. Por exemplo, se você especificar 120 dias, a programação excluirá automaticamente os snapshots do nível de arquivamento quando eles atingirem essa idade.

> **Important**
>
> O período de retenção mínimo para snapshots arquivados é de 90 dias. Você deve especificar uma regra de retenção para reter o snapshot por pelo menos 90 dias.

e. Habilitar a restauração rápida de snapshots.

   Para habilitar a restauração rápida de snapshots para snapshots criados pelo agendamento, na seção Fast snapshot restore (Restauração rápida de snapshots), selecione Enable fast snapshot restore (Habilitar restauração rápida de snapshots). Se você habilitar a restauração rápida de snapshots, deverá escolher as zonas de disponibilidade nas quais serão habilitadas. Se o agendamento usar uma programação de retenção baseada em idade, será necessário especificar o período para o qual habilitar a restauração rápida de snapshots para cada snapshot. Se o agendamento usar retenção baseada em contagem, será necessário especificar o número máximo de snapshots para ativar a restauração rápida de snapshots.

   Se o agendamento criar snapshots em um Outpost, você não poderá habilitar a restauração rápida de snapshots. A restauração rápida de snapshots não é compatível com snapshots locais armazenados em um Outpost.

   > **Note**
   >
   > Você será cobrado por cada minuto em que a restauração rápida de snapshots estiver habilitada para um snapshot em uma determinada zona de disponibilidade. As cobranças são divididas com um mínimo de uma hora.

f. Configurar cópia entre regiões.

   Para copiar snapshots criados pelo agendamento para um Outpost ou para uma região diferente, na seção Cross-Region copy (Cópia entre regiões), selecione Enable cross-Region copy (Habilitar cópia entre regiões).

   Se a política criar snapshots em uma região, será possível copiar os snapshots para até três regiões ou Outposts adicionais em sua conta. Especifique uma regra de cópia entre regiões separada para cada região ou Outpost de destino.

Para cada região ou Outpost, é possível escolher diferentes políticas de retenção e se deseja copiar todas as tags ou nenhuma. Se o snapshot de origem estiver criptografado, ou se a criptografia estiver habilitada por padrão, os snapshots copiados serão criptografados. Se o snapshot de origem não estiver criptografado, será possível habilitar a criptografia. Se você não especificar uma chave do KMS, os snapshots serão criptografados usando a chave do KMS padrão de criptografia do EBS em cada região de destino. Se você especificar uma Chave do KMS para a região de destino, a função do IAM selecionada deverá ter acesso à Chave do KMS.

> **Note**
>
> É necessário garantir que o número de cópias de snapshots simultâneas não seja excedido por região.

Se a política criar snapshots em um Outpost, você não poderá copiá-los para uma região ou outro Outpost e as configurações de cópia entre regiões não estarão disponíveis.

g. Configurar compartilhamento entre contas.

   No compartilhamento entre contas, configure a política para compartilhar automaticamente os instantâneos criados pela agenda com outras AWS contas. Faça o seguinte:

   i. Para ativar o compartilhamento com outras AWS contas, selecione Ativar compartilhamento entre contas.

   ii. Para adicionar contas com as quais os snapshots serão compartilhados, escolha Add account (Adicionar conta), insira o ID de 12 dígitos da conta da AWS e escolha Add (Adicionar).

   iii. Para cancelar o compartilhamento de snapshots compartilhados automaticamente após um período específico, selecione Unshare automatically (Cancelar o compartilhamento automaticamente). Se você escolher cancelar automaticamente o compartilhamento de snapshots compartilhados, o período após o qual cancelar o compartilhamento automaticamente dos snapshots não poderá ser maior do que o período para o qual a política retém seus snapshots. Por exemplo, se a configuração de retenção da política retém snapshots por um período de cinco dias, é possível configurar a política para cancelar o compartilhamento automático

de snapshots compartilhados após períodos de até quatro dias. Isso se aplica a políticas com configurações de retenção de snapshots baseadas em idade e em contagem.

Se você não habilitar o cancelamento automático de compartilhamento, o snapshot será compartilhado até ser excluído.

> **Note**
>
> Você só pode compartilhar snapshots não criptografados ou criptografados usando uma chave gerenciada pelo cliente gerenciada pelo cliente. Você não pode compartilhar snapshots criptografados com a Chave do KMS de criptografia padrão do EBS. Se você compartilhar snapshots criptografados, também deverá compartilhar a Chave do KMS usada para criptografar o volume de origem com as contas de destino. Para obter mais informações, consulte Como permitir que usuários em outras contas usem uma chave do KMS no Guia do desenvolvedor do AWS Key Management Service .

h. Para adicionar outros agendamentos, escolha Add another schedule (Adicionar outro agendamento), localizado na parte superior da tela. Para cada agendamento adicional, preencha os campos conforme descrito anteriormente neste tópico.

i. Depois de adicionar os agendamentos necessárias, escolha Review policy (Revisar política).

12. Revise o resumo da política e escolha Create policy (Criar política).

> **Note**
>
> Se receber um erro `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consulte Solução de problemas para obter mais informações.

Command line

Use o comando create-lifecycle-policy para criar uma política de ciclo de vida de snapshots. Para `PolicyType`, especifique `EBS_SNAPSHOT_MANAGEMENT`.

> **Note**
>
> Para simplificar a sintaxe, os exemplos a seguir usam um arquivo JSON `policyDetails.json`, que inclui os detalhes da política.

Exemplo 1: política de ciclo de vida de snapshot com duas programações

Este exemplo cria uma política de ciclo de vida de snapshot que cria snapshots de todos os volumes que têm uma chave de tag de `costcenter` com um valor de `115`. A política inclui duas programações. A primeira programação cria um snapshot todos os dias às 3h UTC. A segunda programação cria um snapshot semanal todas as sextas-feiras às 17h UTC.

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [{
        "Key": "costcenter",
        "Value": "115"
    }],
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
```

```
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    },
    {
        "Name": "WeeklySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myWeeklySnapshot"
        }],
        "CreateRule": {
            "CronExpression": "cron(0 17 ? * FRI *)"
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

Se a solicitação for bem-sucedida, o comando retornará o ID da política recém-criada. O seguinte é um exemplo de saída.

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

Exemplo 2: política de ciclo de vida de snapshot direcionada a instâncias que cria snapshots de um subconjunto de volumes de dados (não raiz)

Este exemplo cria uma política de ciclo de vida de snapshots de vários volumes com base em instâncias marcadas com `code=production`. A política inclui um agendamento. O agendamento não cria snapshots dos volumes de dados com a etiqueta `code=temp`.

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
```

```
    --policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "code",
        "Value": "production"
    }],
    "Parameters": {
        "ExcludeDataVolumeTags": [{
            "Key": "code",
            "Value": "temp"
        }]
    },
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

Se a solicitação for bem-sucedida, o comando retornará o ID da política recém-criada. O seguinte é um exemplo de saída.

```
{
```

```
    "PolicyId": "policy-0123456789abcdef0"
}
```

Exemplo 3: política de ciclo de vida de snapshots que automatiza snapshots locais de recursos do Outpost

Este exemplo cria uma política de ciclo de vida de snapshots que cria snapshots de volumes marcados com `team=dev` em todos os seus Outposts. A política cria os snapshots nos mesmos Outposts que os volumes de origem. A política cria snapshots a cada 12 horas a partir das `00:00` UTC.

```
aws dlm create-lifecycle-policy \
    --description "My local snapshot policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
 "ResourceLocations": "OUTPOST",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
 "Location": [
  "OUTPOST_LOCAL"
 ]
        },
        "RetainRule": {
            "Count": 1
```

```
        },
        "CopyTags": false
    }
]}
```

Exemplo 4: política de ciclo de vida de snapshots que cria snapshots em uma região e os copia para um Outpost

O exemplo de política a seguir cria snapshots de volumes com a tag `team=dev`. Os snapshots são criados na mesma região que o volume de origem. Os snapshots são criados a cada 12 horas a partir das `00:00` UTC e retêm, no máximo, 1 snapshot. A política também copia os snapshots para o Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`, criptografa os snapshots copiados usando a Chave do KMS de criptografia padrão e retém as cópias por 1 mês.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
    "ResourceLocations": "CLOUD",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CopyTags": false,
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
            "Location": "CLOUD"
```

```
        },
        "RetainRule": {
            "Count": 1
        },
        "CrossRegionCopyRules" : [
        {
            "Target": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0",
            "Encrypted": true,
            "CopyTags": true,
            "RetainRule": {
                "Interval": 1,
                "IntervalUnit": "MONTHS"
            }
        }]
    }
]}
```

Exemplo 5: política de ciclo de vida de snapshots com uma programação baseada em idade habilitada para arquivamento

Este exemplo cria uma política de ciclo de vida de snapshots que visa volumes marcados com `Name=Prod`. A política tem uma programação baseada em idade que cria snapshots no primeiro dia de cada mês às 9h. A programação retém cada snapshot no nível padrão por um dia e depois o move para o nível de arquivamento. Os snapshots são armazenados no nível de arquivamento por 90 dias antes de serem excluídos.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
```

```
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Interval": 1,
          "IntervalUnit": "DAYS"
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Interval": 90,
                 "IntervalUnit": "DAYS"
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Name",
        "Value": "Prod"
      }
    ]
}
```

Exemplo 6: política de ciclo de vida de snapshots com uma programação baseada em conta habilitada para arquivamento

Este exemplo cria uma política de ciclo de vida de snapshots que visa volumes marcados com `Purpose=Test`. A política tem uma programação baseada em contagem que cria snapshots no primeiro dia de cada mês às 9h. A programação arquiva os snapshots imediatamente após a criação e retém no máximo três snapshots no nível de arquivamento.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
```

```
    --policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Count": 0
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Count": 3
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Purpose",
        "Value": "Test"
      }
    ]
}
```

Considerações sobre políticas de ciclo de vida de snapshots

As seguintes considerações gerais se aplicam a políticas de ciclo de vida de snapshot:

- As políticas de ciclo de vida do snapshot visam somente instâncias ou volumes que estão na mesma região que a política.
- A primeira operação de criação de snapshot começa uma hora após o horário de início especificado. As operações subsequentes de criação de snapshot começam uma hora após o horário programado.
- É possível criar várias políticas para fazer backup de um volume ou de uma instância. Por exemplo, se um volume tiver 2 etiquetas, com a etiqueta A como o destino da política A para criar um snapshot a cada 12 horas, e a etiqueta B como o destino da política B para criar um snapshot a cada 24 horas, o Amazon Data Lifecycle Manager cria snapshots de acordo com as programações de ambas as políticas. Como alternativa, é possível obter o mesmo resultado criando uma única política que tenha várias programações. Por exemplo, é possível criar uma única política voltada apenas para tag A e especificar duas programações: uma para cada 12 horas e uma para cada 24 horas.
- Tags de recursos de destino diferenciam letras maiúsculas de minúsculas.
- Se você remover as tags de destino de um recurso visado por uma política, o Amazon Data Lifecycle Manager não gerenciará mais os snapshots existentes no nível padrão e no nível de arquivamento; você deverá excluí-los manualmente se eles não forem mais necessários.
- Se você criar uma política que segmente instâncias e novos volumes forem anexados à instância-alvo após a criação da política, os volumes recém-adicionados serão incluídos no backup na próxima execução da política. Todos os volumes associados à instância no momento da execução da política são incluídos.
- Se você criar uma política com uma programação personalizada baseada em cron que esteja configurada para criar apenas um snapshot, a política não excluirá automaticamente esse snapshot quando o limite de retenção for atingido. Exclua manualmente o snapshot caso ele não seja mais necessário.
- Se você criar uma política baseada na idade em que o período de retenção seja menor do que a frequência de criação, o Amazon Data Lifecycle Manager sempre reterá o último snapshot até que o próximo seja criado. Por exemplo, se uma política baseada na idade criar um snapshot por mês com um período de retenção de sete dias, o Amazon Data Lifecycle Manager reterá cada snapshot por um mês, mesmo que o período de retenção seja de sete dias.

As seguintes considerações se aplicam ao arquivamento de snapshots:

- Você só pode habilitar o arquivamento de snapshots para políticas de snapshots que visem volumes.

- Você só pode especificar uma regra de arquivamento para uma única programação para cada política.
- Se você estiver usando o console, só poderá habilitar o arquivamento de snapshots se a programação tiver uma frequência de criação mensal ou anual, ou tiver uma expressão cron com uma frequência de criação de pelo menos 28 dias.

  Se você estiver usando a AWS API ou o AWS CLI AWS SDK, poderá ativar o arquivamento de instantâneos somente se o cronograma tiver uma expressão cron com uma frequência de criação de pelo menos 28 dias.
- O período mínimo de retenção no nível de arquivamento é de 90 dias.
- Quando um snapshot está arquivado, ele é convertido em um snapshot completo quando é movido para o nível de arquivamento. Isso pode resultar em custos de armazenamento de snapshots mais altos. Para ter mais informações, consulte Definição de preço e faturamento.
- A restauração rápida e o compartilhamento de snapshots são desabilitados para os snapshots quando eles são arquivados.
- Se, no caso de um ano bissexto, a regra de retenção resultar em um período de retenção de arquivos de menos de 90 dias, o Amazon Data Lifecycle Manager garantirá que os snapshots sejam retidos pelo período mínimo de 90 dias.
- Se você arquivar manualmente um snapshot criado pelo Amazon Data Lifecycle Manager e o snapshot ainda estiver arquivado quando o limite de retenção da programação for atingido, o Amazon Data Lifecycle Manager não gerenciará mais esse snapshot. Porém, se você restaurar o snapshot no nível padrão antes que o limite de retenção da programação seja atingido, a programação continuará gerenciando o snapshot de acordo com as regras de retenção.
- Se você restaurar, permanente ou temporariamente, um snapshot arquivado pelo Amazon Data Lifecycle Manager no nível padrão e o snapshot ainda estiver arquivado quando o limite de retenção da programação for atingido, o Amazon Data Lifecycle Manager não gerenciará mais esse snapshot. Porém, se você rearquivar o snapshot antes que o limite de retenção da programação seja atingido, a programação excluirá o snapshot quando o limite de retenção for atingido.
- Os snapshots arquivados pelo Amazon Data Lifecycle Manager contam para as cotas de `Archived snapshots per volume` e `In-progress snapshot archives per account`.
- Se uma programação não conseguir arquivar um snapshot após repetidas tentativas durante 24 horas, o snapshot permanecerá no nível padrão e será programado para exclusão com base na hora em que seria excluído do nível de arquivamento. Por exemplo, se a programação arquivar snapshots por 120 dias, o snapshot permanecerá no nível padrão por 120 dias após a falha

no arquivamento antes de ser excluído permanentemente. Para programações baseadas em contagem, o snapshot não conta para a contagem de retenção da programação.

- Os snapshots devem ser arquivados na mesma região em que foram criados. Se você tiver habilitado a cópia e arquivamento de snapshot entre regiões, o Amazon Data Lifecycle Manager não arquivará a cópia do snapshot.
- Os snapshots arquivados pelo Amazon Data Lifecycle Manager são marcados com a etiqueta `aws:dlm:archived=true` do sistema. Além disso, os snapshots criados por uma programação baseada em idade habilitada para arquivamento são marcados com a tag `aws:dlm:expirationTime` do sistema, que indica a data e a hora em que o snapshot está programado para ser arquivado.

Estas considerações se aplicam a excluir volumes raiz e volumes de dados (não raiz):

- Se você optar por excluir volumes de inicialização e especificar tags que, consequentemente, excluem todos os volumes de dados adicionais anexados a uma instância, o Amazon Data Lifecycle Manager não criará nenhum snapshot para a instância afetada e emitirá uma métrica. `SnapshotsCreateFailed` CloudWatch Para obter mais informações, consulte Monitorar suas políticas usando CloudWatch.

Os seguintes fatores são aplicáveis à exclusão de volumes ou ao encerramento de instâncias com direcionamento por políticas de ciclo de vida de snapshots:

- Se você excluir um volume ou encerrar uma instância visada por uma política com uma programação de retenção baseada em contagem, o Amazon Data Lifecycle Manager não gerenciará mais os snapshots no nível padrão e no nível de arquivamento que foram criados a partir do volume excluído ou da instância encerrada. Exclua manualmente esses snapshots mais antigos caso eles não sejam mais necessários.
- Se você excluir um volume ou encerrar uma instância visada por uma política com uma programação de retenção baseada em idade, a política continuará excluir snapshots no nível padrão e no nível de arquivamento que foram criados a partir do volume ou da instância excluídos até restar apenas um snapshot. Exclua manualmente o último snapshot caso ele não seja mais necessário.

As seguintes considerações se aplicam às políticas de ciclo de vida de snapshots e à restauração rápida de snapshots:

- O Amazon Data Lifecycle Manager pode habilitar a restauração rápida de snapshots somente para snapshots com um tamanho de 16 TiB ou menos. Para ter mais informações, consulte Restauração rápida de snapshots do Amazon EBS.
- Um snapshot habilitado para restauração rápida continua habilitado mesmo que você exclua ou desabilite a política, desabilite a restauração rápida de snapshots ou desabilite a restauração de snapshots para a zona de disponibilidade. É possível desabilitar a restauração rápida desses snapshots manualmente.
- Se você habilitar a restauração rápida de snapshots para uma política e exceder o número máximo de snapshots que podem ser habilitados para restauração rápida de snapshots, o Amazon Data Lifecycle Manager criará snapshots, mas não os habilitará para restauração rápida. Depois que um snapshot que está habilitado para restauração rápida for excluído, o próximo snapshot que o Amazon Data Lifecycle Manager criar será habilitado para restauração rápida.
- Quando a restauração rápida de um snapshot é habilitada, são necessários 60 minutos por TiB para otimizar o snapshot. Recomendamos configurar as programações de modo que cada snapshot seja totalmente otimizado antes que o Amazon Data Lifecycle Manager crie o próximo snapshot.
- Se você habilitar a restauração rápida de snapshots para uma política que visa instâncias, o Amazon Data Lifecycle Manager habilitará a restauração rápida de snapshot para cada um dos snapshots de vários volumes, definidos individualmente. Se o Amazon Data Lifecycle Manager não habilitar a restauração rápida de snapshots para um dos snapshots no conjunto de snapshots de vários volumes, ele tentará habilitar a restauração rápida para os snapshots restantes no conjunto.
- Você será cobrado por cada minuto em que a restauração rápida de snapshots estiver habilitada para um snapshot em uma determinada zona de disponibilidade. As cobranças são divididas com um mínimo de uma hora. Para ter mais informações, consulte Definição de preço e cobrança.

> **Note**
>
> Dependendo da configuração de suas políticas de ciclo de vida, é possível ter vários snapshots habilitados para restauração rápida de snapshots em várias zonas de disponibilidade, simultaneamente.

As considerações a seguir se aplicam às políticas de ciclo de vida de snapshots e aos volumes habilitados para multi-attach:

- Ao criar uma política de ciclo de vida voltada para instâncias que tenham o mesmo volume habilitado de Multi-Attach, o Amazon Data Lifecycle Manager inicia um snapshot do volume para cada instância anexada. Use a tag timestamp para identificar o conjunto de snapshots consistentes em relação ao tempo criados das instâncias anexadas.

As considerações a seguir se aplicam ao compartilhamento de snapshots entre contas:

- Você só pode compartilhar snapshots não criptografados ou criptografados usando uma chave gerenciada pelo cliente gerenciada pelo cliente.
- Você não pode compartilhar snapshots criptografados com a Chave do KMS de criptografia padrão do EBS.
- Se você compartilhar snapshots criptografados, também deverá compartilhar a chave do KMS usada para criptografar o volume de origem com as contas de destino. Para obter mais informações, consulte Como permitir que usuários em outras contas usem uma chave do KMS no Guia do desenvolvedor do AWS Key Management Service .

As considerações a seguir se aplicam às políticas de snapshots e ao arquivamento de snapshots:

- Se você arquivar manualmente um snapshot criado por uma política e esse snapshot estiver no nível de arquivamento quando o limite de retenção da política for atingido, o Amazon Data Lifecycle Manager não excluirá o snapshot. O Amazon Data Lifecycle Manager não gerencia snapshots enquanto eles são armazenados no nível de arquivamento. Se não precisar mais dos snapshots que estão armazenados no nível de arquivamento, você deve excluí-los manualmente.

As seguintes considerações se aplicam às políticas de snapshots e à Lixeira:

- Se o Amazon Data Lifecycle Manager excluir um snapshot e enviá-lo para a lixeira quando o limite de retenção da política for atingido e você restaurar manualmente o snapshot da lixeira, você deverá excluir manualmente esse snapshot quando ele não for mais necessário. O Amazon Data Lifecycle Manager não poderá mais gerenciar o snapshot.
- Se você excluir manualmente um snapshot criado por uma política e esse snapshot estiver na lixeira quando o limite de retenção da política for atingido, o Amazon Data Lifecycle Manager não excluirá o snapshot. O Amazon Data Lifecycle Manager não gerencia snapshots enquanto eles estão armazenados no nível de arquivamento.

Se o snapshot for restaurado da lixeira antes que o limite de retenção da política seja atingido, o Amazon Data Lifecycle Manager excluirá o snapshot quando o limite de retenção da política for atingido.

Se o snapshot for restaurado da lixeira depois que o limite de retenção da política seja atingido, o Amazon Data Lifecycle Manager não excluirá mais o snapshot. Exclua manualmente o snapshot quando ele não for mais necessário.

As seguintes considerações se aplicam a políticas de ciclo de vida de snapshots que estão no estado error:

- Para políticas com programações de retenção com base na idade, os snapshots configurados para expirar enquanto a política estiver no estado `error` serão retidos por tempo indeterminado. Será necessário excluir os snapshots manualmente. Quando você habilita a política novamente, o Amazon Data Lifecycle Manager retoma a exclusão de snapshots à medida que os períodos de retenção expiram.
- Para políticas com programas de retenção com base em contagem, a política interrompe a criação e exclusão de snapshtos enquanto está no estado `error`. Ao reabilitar a política, o Amazon Data Lifecycle Manager retoma a criação de snapshots e retoma a exclusão de snapshots quando o limite de retenção é atingido.

As seguintes considerações se aplicam às políticas de snapshot e bloqueio de snapshot:

- Se você bloquear manualmente um snapshot criado pelo Amazon Data Lifecycle Manager e esse snapshot ainda estiver bloqueado quando seu limite de retenção for atingido, o Amazon Data Lifecycle Manager não gerenciará mais esse snapshot. Exclua manualmente o snapshot caso ele não seja mais necessário.
- Se você bloquear manualmente um snapshot criado e habilitado para restauração rápida de snapshots pelo Amazon Data Lifecycle Manager e o snapshot ainda estiver arquivado quando seu limite de retenção for atingido, o Amazon Data Lifecycle Manager não desabilitará a restauração rápida de snapshots nem excluirá o snapshot. Você deve desabilitar manualmente a restauração rápida de snapshots e excluir o snapshot caso ele não seja mais necessário.
- Se você registrar manualmente um snapshot criado por Amazon Data Lifecycle Manager com uma AMI e depois bloquear o snapshot e ele ainda estiver bloqueado e associado à AMI quando seu limite de retenção for atingido, o Amazon Data Lifecycle Manager continuará tentando excluir o

snapshot. Quando o registro da AMI for cancelado e o snapshot for desbloqueado, o Amazon Data Lifecycle Manager excluirá automaticamente o snapshot.

Recursos adicionais do

Para obter mais informações, consulte o blog Automatizando o snapshot e o gerenciamento de AMI do Amazon EBS usando o Amazon AWS Data Lifecycle Manager.

Requisitos para o uso de scripts prévios e posteriores

A tabela a seguir descreve os requisitos para o uso de scripts prévios e posteriores com o Amazon Data Lifecycle Manager.

	Snapshots consistentes com aplicação		
Requisito	Backup do VSS	Documento do SSM personalizado	Outros casos de uso
Agente SSM instalado e em execução nas instâncias de destino	✓	✓	✓
Requisitos do sistema VSS atendidos nas instâncias de destino	✓		
Perfil de instância habilitado para VSS associado às instâncias de destino	✓		
Componentes do VSS instalados nas instâncias de destino	✓		
Prepare o documento SSM com comandos pré e pós-script		✓	✓

	Snapshots consistentes com aplicação		
Prepare a função IAM do Amazon Data Lifecycle Manager, execute scripts anteriores e posteriores	✓	✓	✓
Crie uma política de snapshot que vise instâncias e seja configurada para scripts anteriores e posteriores	✓	✓	✓

Automatizar snapshots consistentes com a aplicação com scripts prévios e posteriores

Você pode automatizar snapshots consistentes com a aplicação com o Amazon Data Lifecycle Manager habilitando scripts prévios e posteriores nas políticas de ciclo de vida de snapshot que têm as instâncias como alvo.

O Amazon Data Lifecycle Manager se integra ao (Systems AWS Systems Manager Manager) para oferecer suporte a snapshots consistentes com aplicativos. O Amazon Data Lifecycle Manager usa documentos de comando do Systems Manager (SSM) que incluem scripts prévios e posteriores para automatizar as ações necessárias para fazer snapshots consistentes com a aplicação. Antes de iniciar a criação de snapshots, o Amazon Data Lifecycle Manager executa os comandos do script prévio para congelar e despejar a E/S. Depois que o Amazon Data Lifecycle Manager inicia a criação de snapshots, ele executa os comandos do script posterior para descongelar a E/S.

Usando o Amazon Data Lifecycle Manager, você pode automatizar os snapshots consistentes com a aplicação dos seguintes itens:

- Aplicações do Windows que usam o Volume Shadow Copy Service (VSS)
- SAP HANA usando um documento AWS SSDM gerenciado. Para obter mais informações, consulte Amazon EBS snapshots for SAP HANA.

- Bancos de dados autogerenciados, como MySQL, PostgreSQL ou IRIS, usando modelos de documentos SSM InterSystems

Tópicos

Conceitos básicos dos snapshots consistentes com a aplicação

Esta seção explica as etapas que você precisa seguir para automatizar snapshots consistentes com a aplicação usando o Amazon Data Lifecycle Manager.

Etapa 1: preparar as instâncias-alvo

Você precisa preparar as instâncias-alvo para snapshots consistentes com a aplicação usando o Amazon Data Lifecycle Manager. Dependendo do caso de uso, faça um dos procedimentos a seguir.

Prepare for VSS Backups

Para preparar as instâncias-alvo para backups do VSS

1. Instale o SSM Agent nas instâncias-alvo, se ainda não estiver instalado. Se o SSM Agent já estiver instalado em suas instâncias-alvo, pule esta etapa.

   Para obter mais informações, consulte Instalar o SSM Agent manualmente em instâncias do Amazon EC2 para Windows .
2. Certifique-se de que o SSM Agent esteja em execução. Para obter mais informações, consulte Verificar o status do SSM Agent e iniciar o agente.
3. Configure o Systems Manager para instâncias do Amazon EC2. Para obter mais informações, consulte Configuração do Systems Manager para instâncias Amazon EC2 no AWS Systems Manager Guia do usuário do .
4. Certifique-se de que os requisitos do sistema para backups do VSS sejam atendidos.
5. Anexe um perfil de instância habilitado para o VSS às instâncias-alvo.
6. Instale os componentes do VSS.

Prepare for SAP HANA backups

Para preparar as instâncias-alvo para backups do SAP HANA

1. Prepare o ambiente do SAP HANA nas instâncias-alvo.

   a. Configure a instância com o SAP HANA. Se você ainda não tiver um ambiente do SAP HANA, pode consultar SAP HANA Environment Setup on AWS.

   b. Faça login no SystemDB como um usuário administrador adequado.

   c. Crie um usuário de backup de banco de dados para ser usado com o Amazon Data Lifecycle Manager.

   ```
   CREATE USER username PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
   ```

   Por exemplo, o comando a seguir criar um usuário denominado `dlm_user` com a senha `password`.

   ```
   CREATE USER dlm_user PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
   ```

   d. Atribua um perfil de `BACKUP OPERATOR` ao usuário de backup do banco de dados que você criou na etapa anterior.

   ```
   GRANT BACKUP OPERATOR TO username
   ```

   Por exemplo, o comando a seguir atribui o perfil a um usuário denominado `dlm_user`.

   ```
   GRANT BACKUP OPERATOR TO dlm_user
   ```

   e. Faça login no sistema operacional como administrador, por exemplo *sid*`adm`.

   f. Crie uma entrada `hdbuserstore` para armazenar as informações de conexão para que o documento do SSM do SAP HANA possa se conectar ao SAP HANA sem que os usuários precisem inserir as informações.

   ```
   hdbuserstore set DLM_HANADB_SNAPSHOT_USER
    localhost:3hana_instance_number13 username password
   ```

   Por exemplo: .

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER localhost:30013 dlm_user password
```

g. Teste a conexão.

```
hdbsql -U DLM_HANADB_SNAPSHOT_USER "select * from dummy"
```

2. Instale o SSM Agent nas instâncias-alvo, se ainda não estiver instalado. Se o SSM Agent já estiver instalado em suas instâncias-alvo, pule esta etapa.

   Para obter mais informações, consulte Instalar o SSM Agent manualmente em instâncias do Amazon EC2 para Linux.

3. Certifique-se de que o SSM Agent esteja em execução. Para obter mais informações, consulte Verificar o status do SSM Agent e iniciar o agente.
4. Configure o Systems Manager para instâncias do Amazon EC2. Para obter mais informações, consulte Configuração do Systems Manager para instâncias Amazon EC2 no AWS Systems Manager Guia do usuário do .

Prepare for custom SSM documents

Para preparar os documentos do SSM personalizados das instâncias-alvo

1. Instale o SSM Agent nas instâncias-alvo, se ainda não estiver instalado. Se o SSM Agent já estiver instalado em suas instâncias-alvo, pule esta etapa.
   - (Instâncias do Linux) Instalar o SSM Agent manualmente em instâncias do Amazon EC2 para Linux
   - (Instâncias do Windows) Instalar o SSM Agent manualmente em instâncias do Amazon EC2 para Windows
2. Certifique-se de que o SSM Agent esteja em execução. Para obter mais informações, consulte Verificar o status do SSM Agent e iniciar o agente.
3. Configure o Systems Manager para instâncias do Amazon EC2. Para obter mais informações, consulte Configuração do Systems Manager para instâncias Amazon EC2 no AWS Systems Manager Guia do usuário do .

Etapa 2: preparar o documento do SSM

> **Note**
>
> Essa etapa só é necessária para documentos do SSM personalizados. Não é necessária para backup do VSS ou para o SAP HANA. Para backups do VSS e SAP HANA, o Amazon Data Lifecycle Manager AWS usa o documento SSM gerenciado.

Se você estiver automatizando instantâneos consistentes com aplicativos para um banco de dados autogerenciado, como MySQL, PostgreSQL InterSystems ou IRIS, deverá criar um documento de comando SSM que inclua um pré-script para congelar e liberar a E/S antes do início da criação do instantâneo e um pós-script para descongelar a E/S após o início da criação do instantâneo.

Se seu banco de dados MySQL, PostgreSQL ou InterSystems IRIS usa configurações padrão, você pode criar um documento de comando SSM usando o conteúdo de amostra do documento SSM abaixo. Se seu banco de dados MySQL, PostgreSQL ou InterSystems IRIS usa uma configuração não padrão, você pode usar o conteúdo de amostra abaixo como ponto de partida para seu documento de comando SSM e depois personalizá-lo para atender às suas necessidades. Ou então, se quiser criar um novo documento do SSM começando do zero, você pode usar o modelo de documento do SSM em branco abaixo e adicionar seus comandos prévios e posteriores nas seções apropriadas do documento.

> **Observe o seguinte:**
>
> - É sua responsabilidade garantir que o documento do SSM realize as ações corretas e necessárias para a configuração do banco de dados.
> - Só haverá garantia de que os snapshots sejam consistentes com a aplicação se os scripts prévios e posteriores no documento do SSM puderem congelar, descarregar e descongelar a E/S com sucesso.
> - O documento do SSM deve incluir os campos obrigatórios para `allowedValues`, incluindo `pre-script`, `post-script` e `dry-run`. O Amazon Data Lifecycle Manager executará os comandos na instância com base no conteúdo dessas seções. Se o documento do SSM não tiver essas seções, o Amazon Data Lifecycle Manager o tratará como uma execução que falhou.

MySQL sample document content

```
###============================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###============================================================================###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for MySQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
```

```
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run MySQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
      ### Error Codes

 ###============================================================================###
      # The following Error codes will inform Data Lifecycle Manager of the type of
 error
      # and help guide handling of the error.
      # The Error code will also be emitted via AWS Eventbridge events in the
 'cause' field.
      # 1 Pre-script failed during execution - 201
      # 2 Post-script failed during execution - 202
      # 3 Auto thaw occurred before post-script was initiated - 203
      # 4 Pre-script initiated while post-script was expected - 204
      # 5 Post-script initiated while pre-script was expected - 205
      # 6 Application not ready for pre or post-script initiation - 206

      ###==================================================================###
      ### Global variables
      ###==================================================================###
      START=$(date +%s)
      # For testing this script locally, replace the below with OPERATION=$1.
      OPERATION={{ command }}
      FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
      FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
      FS_BUSY_ERROR='mount point is busy'
```

```
     # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
     # duration specified in the global variable below. Choose the duration based
on your
     # database application's tolerance to freeze.
     export AUTO_THAW_DURATION_SECS="60"

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
         # Check if filesystem is already frozen. No error code indicates that
filesystem
         # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
         check_fs_freeze
         # Execute the DB commands to flush the DB in preparation for snapshot
         snap_db
         # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
         freeze_fs

         echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
         $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
     }

     # Add all post-script actions to be performed within the function below
     execute_post_script() {
         echo "INFO: Start execution of post-script"
         # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen.
         unfreeze_fs
         thaw_db
     }

     # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
     # in the AUTO_THAW_DURATION_SECS global variable.
     execute_schedule_auto_thaw() {
         sleep ${AUTO_THAW_DURATION_SECS}
         execute_post_script
     }

     # Disable Auto Thaw if it is still enabled
```

```
     execute_disable_auto_thaw() {
         echo "INFO: Attempting to disable auto thaw if enabled"
         auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
         if [ -n "${auto_thaw_pgid}" ]; then
             echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
             sudo pkill -g ${auto_thaw_pgid}
             rc=$?
             if [ ${rc} != 0 ]; then
                 echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
             else
                 echo "INFO: Auto Thaw  has been disabled"
             fi
         fi
     }

     # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
     # Return error code 204 if any of the mount points are already frozen.
     check_fs_freeze() {
         for target in $(lsblk -nlo MOUNTPOINTS)
         do
             # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
             # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
             if [ $target == '/' ]; then continue; fi
             if [[ "$target" == *"/boot"* ]]; then continue; fi

             error_message=$(sudo mount -o remount,noatime $target 2>&1)
             # Remount will be a no-op without a error message if the filesystem is
unfrozen.
             # However, if filesystem is already frozen, remount will fail with
busy error message.
             if [ $? -ne 0 ];then
                 # If the filesystem is already in frozen, return error code 204
                 if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                     echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                     exit 204
                 fi
```

```
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Freezing $target"
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    sudo mysql -e 'UNLOCK TABLES;'
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                thaw_db
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
```

```
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
            fi
            echo "INFO: Thaw complete on $target"
        done
    }

    snap_db() {
        # Run the flush command only when MySQL DB service is up and running
        sudo systemctl is-active --quiet mysqld.service
        if [ $? -eq 0 ]; then
            echo "INFO: Execute MySQL Flush and Lock command."
            sudo mysql -e 'FLUSH TABLES WITH READ LOCK;'
            # If the MySQL Flush and Lock command did not succeed, return error
code 201 to indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: MySQL FLUSH TABLES WITH READ LOCK command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Flush and Lock command."
        fi
    }
```

```
     thaw_db() {
         # Run the unlock command only when MySQL DB service is up and running
         sudo systemctl is-active --quiet mysqld.service
         if [ $? -eq 0 ]; then
             echo "INFO: Execute MySQL Unlock"
             sudo mysql -e 'UNLOCK TABLES;'
         else
             echo "INFO: MySQL service is inactive. Skipping execution of MySQL
 Unlock command."
         fi
     }

     export -f execute_schedule_auto_thaw
     export -f execute_post_script
     export -f unfreeze_fs
     export -f thaw_db

     # Debug logging for parameters passed to the SSM document
     echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

     # Based on the command parameter value execute the function that supports
     # pre-script/post-script operation
     case ${OPERATION} in
         pre-script)
             execute_pre_script
             ;;
         post-script)
             execute_post_script
             execute_disable_auto_thaw
             ;;
         dry-run)
             echo "INFO: dry-run option invoked - taking no action"
             ;;
         *)
             echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
             exit 1 # return failure
             ;;
     esac

     END=$(date +%s)
     # Debug Log for profiling the script time
```

```
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

PostgreSQL sample document content

```
###============================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###============================================================================###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for PostgreSQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
```

```
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run PostgreSQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###==============================================================================###
      ### Error Codes

 ###==============================================================================###
      # The following Error codes will inform Data Lifecycle Manager of the type of
 error
      # and help guide handling of the error.
      # The Error code will also be emitted via AWS Eventbridge events in the
 'cause' field.
      # 1 Pre-script failed during execution - 201
      # 2 Post-script failed during execution - 202
      # 3 Auto thaw occurred before post-script was initiated - 203
      # 4 Pre-script initiated while post-script was expected - 204
      # 5 Post-script initiated while pre-script was expected - 205
      # 6 Application not ready for pre or post-script initiation - 206


 ###==============================================================================###
      ### Global variables

 ###==============================================================================###
      START=$(date +%s)
```

```
     OPERATION={{ command }}
     FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
     FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
     FS_BUSY_ERROR='mount point is busy'

     # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
     # duration specified in the global variable below. Choose the duration based
on your
     # database application's tolerance to freeze.
     export AUTO_THAW_DURATION_SECS="60"

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
         # Check if filesystem is already frozen. No error code indicates that
filesystem
         # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
         check_fs_freeze
         # Execute the DB commands to flush the DB in preparation for snapshot
         snap_db
         # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
         freeze_fs

         echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
         $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
     }

     # Add all post-script actions to be performed within the function below
     execute_post_script() {
         echo "INFO: Start execution of post-script"
         # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen
         unfreeze_fs
     }

     # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
     # in the AUTO_THAW_DURATION_SECS global variable.
     execute_schedule_auto_thaw() {
         sleep ${AUTO_THAW_DURATION_SECS}
```

```
        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
```

```
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Freezing $target"
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
```

```
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
            fi
            echo "INFO: Thaw complete on $target"
        done
    }

    snap_db() {
        # Run the flush command only when PostgreSQL DB service is up and running
        sudo systemctl is-active --quiet postgresql
        if [ $? -eq 0 ]; then
            echo "INFO: Execute Postgres CHECKPOINT"
            # PostgreSQL command to flush the transactions in memory to disk
            sudo -u postgres psql -c 'CHECKPOINT;'
            # If the PostgreSQL Command did not succeed, return error code 201 to
indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: Postgres CHECKPOINT command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: PostgreSQL service is inactive. Skipping execution of
CHECKPOINT command."
```

```
        fi
    }

    export -f execute_schedule_auto_thaw
    export -f execute_post_script
    export -f unfreeze_fs

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            execute_disable_auto_thaw
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
            echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
            exit 1 # return failure
            ;;
    esac

    END=$(date +%s)
    # Debug Log for profiling the script time
    echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

InterSystems IRIS sample document content

```
###============================================================================###
# MIT License
#
# Copyright (c) 2024 InterSystems
#
```

```
# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to deal
# in the Software without restriction, including without limitation the rights
# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in all
# copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
# OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
# SOFTWARE.
###==============================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature for InterSystems IRIS.
parameters:
  executionId:
    type: String
    default: None
    description: Specifies the unique identifier associated with a pre and/or post
 execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
    type: String
    # Data Lifecycle Manager will trigger the pre-script and post-script actions.
 You can also use this SSM document with 'dry-run' for manual testing purposes.
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    #The following allowedValues will allow Data Lifecycle Manager to successfully
 trigger pre and post script actions.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
```

```
- action: aws:runShellScript
  description: Run InterSystems IRIS Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash

 ###==============================================================================###
      ### Global variables

 ###==============================================================================###
      DOCKER_NAME=iris
      LOGDIR=./
      EXIT_CODE=0
      OPERATION={{ command }}
      START=$(date +%s)

      # Check if Docker is installed
      # By default if Docker is present, script assumes that InterSystems IRIS is
 running in Docker
      # Leave only the else block DOCKER_EXEC line, if you run InterSystems IRIS
 non-containerised (and Docker is present).
      # Script assumes irissys user has OS auth enabled, change the OS user or
 supply login/password depending on your configuration.
      if command -v docker &> /dev/null
      then
        DOCKER_EXEC="docker exec $DOCKER_NAME"
      else
        DOCKER_EXEC="sudo -i -u irissys"
      fi


      # Add all pre-script actions to be performed within the function below
      execute_pre_script() {
        echo "INFO: Start execution of pre-script"

        # find all iris running instances
        iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
 '^up' | cut -c5-  | awk '{print $1}')
```

```
        echo "`date`: Running iris instances $iris_instances"

        # Only for running instances
        for INST in $iris_instances; do

          echo "`date`: Attempting to freeze $INST"

          # Detailed instances specific log
          LOGFILE=$LOGDIR/$INST-pre_post.log

          #check Freeze status before starting
          $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).IsWDSuspendedExt()"
          freeze_status=$?
          if [ $freeze_status -eq 5 ]; then
            echo "`date`:   ERROR: $INST IS already FROZEN"
            EXIT_CODE=204
          else
            echo "`date`:   $INST is not frozen"
            # Freeze
            # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
            $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).ExternalFreeze(\"$LOGFILE\",,,,,,600,,,300)"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS FROZEN"
                ;;
              3) echo "`date`:   $INST FREEZE FAILED"
                EXIT_CODE=201
                ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                EXIT_CODE=201
                ;;
            esac
            echo "`date`:   Completed freeze of $INST"
          fi
        done
        echo "`date`: Pre freeze script finished"
      }

      # Add all post-script actions to be performed within the function below
      execute_post_script() {
```

```
        echo "INFO: Start execution of post-script"

        # find all iris running instances
        iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
 '^up' | cut -c5-  | awk '{print $1}')
        echo "`date`: Running iris instances $iris_instances"

        # Only for running instances
        for INST in $iris_instances; do

          echo "`date`: Attempting to thaw $INST"

          # Detailed instances specific log
          LOGFILE=$LOGDIR/$INST-pre_post.log

          #check Freeze status befor starting
          $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).IsWDSuspendedExt()"
          freeze_status=$?
          if [ $freeze_status -eq 5 ]; then
            echo "`date`:  $INST is in frozen state"
            # Thaw
            # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
            $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalThaw(\"$LOGFILE\")"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS THAWED"
                  $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalSetHistory(\"$LOGFILE\")"
                ;;
              3) echo "`date`:   $INST THAW FAILED"
                  EXIT_CODE=202
                ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                  EXIT_CODE=202
                ;;
            esac
            echo "`date`:   Completed thaw of $INST"
          else
            echo "`date`:   ERROR: $INST IS already THAWED"
            EXIT_CODE=205
```

```
          fi
        done
        echo "`date`: Post thaw script finished"
      }

      # Debug logging for parameters passed to the SSM document
        echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

      # Based on the command parameter value execute the function that supports
      # pre-script/post-script operation
      case ${OPERATION} in
        pre-script)
          execute_pre_script
          ;;
        post-script)
          execute_post_script
            ;;
        dry-run)
          echo "INFO: dry-run option invoked - taking no action"
          ;;
        *)
          echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
          # return failure
          EXIT_CODE=1
          ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
      exit $EXIT_CODE
```

Para obter mais informações, consulte o GitHub repositório.

Empty document template

```
###============================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
```

```
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###============================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
```

```
 description: Run Database freeze/thaw commands
 name: run_pre_post_scripts
 precondition:
   StringEquals:
   - platformType
   - Linux
 inputs:
   runCommand:
   - |
     #!/bin/bash


###==============================================================================###
     ### Error Codes

###==============================================================================###
     # The following Error codes will inform Data Lifecycle Manager of the type of
error
     # and help guide handling of the error.
     # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
     # 1 Pre-script failed during execution - 201
     # 2 Post-script failed during execution - 202
     # 3 Auto thaw occurred before post-script was initiated - 203
     # 4 Pre-script initiated while post-script was expected - 204
     # 5 Post-script initiated while pre-script was expected - 205
     # 6 Application not ready for pre or post-script initiation - 206


###==============================================================================###
     ### Global variables

###==============================================================================###
     START=$(date +%s)
     # For testing this script locally, replace the below with OPERATION=$1.
     OPERATION={{ command }}

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
     }

     # Add all post-script actions to be performed within the function below
     execute_post_script() {
```

```
        echo "INFO: Start execution of post-script"
    }

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
            echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
            exit 1 # return failure
            ;;
    esac

    END=$(date +%s)
    # Debug Log for profiling the script time
    echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

Quando tiver o conteúdo do documento do SSM, use um dos procedimentos a seguir para criar o documento do SSM personalizado.

Console

Para criar um documento de comando do SSM

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com//systems-manager/.

2. No painel de navegação, escolha Documentos e depois Criar documento, Comando ou Sessão.
3. Em Name (Nome), insira um nome descritivo para o documento.
4. Em Tipo de destino, selecione/AWS::EC2::Instance.
5. Para Tipo de documento, selecione Comando.
6. No campo Conteúdo, selecione YAML e cole o conteúdo do documento.
7. Na seção Tags do documento, adicione uma tag com uma chave de tag de `DLMScriptsAccess` e um valor de tag de `true`.

> **Important**
>
> A `DLMScriptsAccess:true` tag é exigida pela política AWSDataLifecycleManagerSSMFullAccess AWS gerenciada usada na Etapa 3: Preparar a função IAM do Amazon Data Lifecycle Manager. A política usa a chave de condição `aws:ResourceTag` para restringir o acesso aos documentos do SSM que tenham essa tag.

8. Escolha Criar documento.

AWS CLI

Para criar um documento de comando do SSM

Use o comando create-document. Para `--name`, especifique um nome descritivo para o documento. Em `--document-type`, especifique `Command`. Para `--content`, especifique o caminho para o arquivo .yaml com o conteúdo do documento do SSM. Em `--tags`, especifique `"Key=DLMScriptsAccess,Value=true"`.

```
$ aws ssm create-document \
--content file://path/to/file/documentContent.yaml \
--name "document_name" \
--document-type "Command" \
--document-format YAML \
--tags "Key=DLMScriptsAccess,Value=true"
```

Etapa 3: preparar o perfil do IAM do Amazon Data Lifecycle Manager

> **Note**
>
> Essa etapa é necessária se:
>
> - Você criar ou atualizar uma política de snapshot habilitada para script prévio/posterior que usa um perfil do IAM personalizado.
> - Você usar a linha de comando para criar ou atualizar uma política de snapshot habilitado para script prévio/posterior.
>
> Se você usar o console para criar ou atualizar uma política de instantâneos ativada antes e depois do script que usa a função padrão para gerenciar snapshots () AWSDataLifecycleManagerDefaultRole, pule esta etapa. Nesse caso, anexamos automaticamente a AWSDataLifecycleManagerSSMFullAccesspolítica a essa função.

Você deve garantir que o perfil do IAM que você usa para a política conceda ao Amazon Data Lifecycle Manager permissão para realizar as ações do SSM necessárias para executar scripts prévios e posteriores nas instâncias-alvo da política.

O Amazon Data Lifecycle Manager fornece uma política gerenciada (AWSDataLifecycleManagerSSMFullAccess) que inclui as permissões necessárias. Você pode anexar essa política ao perfil do IAM para gerenciar snapshots e garantir que ela inclua as permissões.

> **Important**
>
> A política AWSDataLifecycleManagerSSMFullAccess gerenciada usa a chave de `aws:ResourceTag` condição para restringir o acesso a documentos SSM específicos ao usar scripts anteriores e posteriores. Para permitir que o Amazon Data Lifecycle Manager acesse os documentos do SSM, você deve garantir que eles estejam marcados com `DLMScriptsAccess:true`.

Ou então, você pode criar manualmente uma política personalizada ou atribuir as permissões necessárias diretamente ao perfil do IAM que você usa. Você pode usar as mesmas permissões definidas na política AWSDataLifecycleManagerSSMFullAccess gerenciada, no entanto, a chave de

`aws:ResourceTag` condição é opcional. Se você decidir não incluir essa chave de condição, não precisará marcar os documentos do SSM com `DLMScriptsAccess:true`.

Use um dos métodos a seguir para adicionar a AWSDataLifecycleManagerSSMFullAccesspolítica à sua função do IAM.

Console

Para anexar a política gerenciada ao seu perfil personalizado

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Roles (Funções).
3. Pesquise e selecione o perfil personalizado para gerenciar os snapshots.
4. Na guia Permissões, escolha Adicionar permissões, Anexar políticas.
5. Pesquise e selecione a política AWSDataLifecycleManagerSSMFullAccessgerenciada e, em seguida, escolha Adicionar permissões.

AWS CLI

Para anexar a política gerenciada ao seu perfil personalizado

Use o comando attach-role-policy. Para `---role-name`, especifique o nome do seu perfil personalizado. Em `--policy-arn`, especifique `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`.

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Etapa 4: criar uma política de ciclo de vida de snapshots

Para automatizar snapshots consistentes com a aplicação, você deve criar uma política de ciclo de vida de snapshots que tenha como alvo as instâncias e configurar scripts prévios e posteriores para essa política.

Console

Para criar uma política de ciclo de vida de snapshots

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Na tela Select policy type (Selecionar tipo de política), escolha EBS snapshot policy (Política de snapshot do EBS) e depois Next (Próximo).
4. Na seção Target resources (Recursos de destino), faça o seguinte:
   a. Para Tipos de recursos-alvo, escolha `Instance`.
   b. Para Tags de recurso-alvo, especifique as tags de recurso que identificam as instâncias para backup. Só será feito backup dos recursos que têm as tags especificadas.
5. Para a função do IAM, escolha AWSDataLifecycleManagerDefaultRole(a função padrão para gerenciar instantâneos) ou escolha uma função personalizada que você criou e preparou para scripts anteriores e posteriores.
6. Configure as agendas e as opções adicionais conforme necessário. Recomendamos que você agende a criação dos snapshots para períodos que atendam à sua workload, como durante janelas de manutenção.

   No SAP HANA, recomendamos que você habilite a restauração rápida de snapshots.

   > **Note**
   > Se você habilitar uma agenda para backups do VSS, não poderá habilitar Excluir volumes de dados específicos ou Copiar tags da fonte.

7. Na seção Scripts prévios e posteriores, selecione Habilitar scripts prévios e posteriores e depois, dependendo da sua workload, faça o seguinte:
   - Para criar snapshots consistentes com a aplicação para as aplicações do Windows, selecione Backup do VSS.
   - Para criar snapshots consistentes com a aplicação de suas workloads do SAP HANA, selecione SAP HANA.
   - Para criar instantâneos consistentes com aplicativos de todos os outros bancos de dados e cargas de trabalho, incluindo seus bancos de dados MySQL, PostgreSQL InterSystems ou

IRIS autogerenciados, usando um documento SSM personalizado, selecione Documento SSM personalizado.

1. Para Opção de automatização, escolha Scripts prévios e posteriores.
2. Para Documento do SSM, selecione o documento do SSM que você preparou.

8. Dependendo da opção selecionada, configure as seguintes opções adicionais:

   - Tempo limite do script: (somente documento do SSM personalizado) O tempo limite após o qual o Amazon Data Lifecycle Manager considera que a tentativa de execução do script falhou se não foi concluída. Se um script não for concluído dentro do período limite, o Amazon Data Lifecycle Manager considerará que a tentativa falhou. O período de tempo limite se aplica aos scripts prévios e posteriores individualmente. O limite de tempo mínimo e padrão é de 10 segundos. E o tempo limite máximo é de 120 segundos.
   - Tentar os scripts com falha novamente: selecione essa opção para fazer novas tentativas de executar os scripts que não forem concluídos dentro do período de tempo limite. Se o script prévio falhar, o Amazon Data Lifecycle Manager tentará realizar novamente todo o processo de criação de snapshots, incluindo a execução dos scripts prévios e posteriores. Se o script posterior falhar, o Amazon Data Lifecycle Manager fará nova tentativa de executar apenas o script posterior; nesse caso, o script prévio estará sido concluído e o snapshot poderá ter sido criado.
   - Usar o padrão de snapshots consistentes em caso de falha: selecione essa opção para usar padrão de snapshots consistentes em caso de falha se a execução do script prévio falhar. Esse é o comportamento padrão da criação de snapshots para o Amazon Data Lifecycle Manager se os scripts prévios e posteriores não estiverem habilitados. Se você habilitou novas tentativas, o Amazon Data Lifecycle Manager só usará o padrão de snapshots consistentes em caso de falha após esgotar o todas as tentativas. Se o script prévio falhar e você não usar o padrão de snapshots consistentes em caso de falha, o Amazon Data Lifecycle Manager não criará snapshots para a instância durante da execução agendada.

   > **Note**
   >
   > Se você estiver criando snapshots para o SAP HANA, talvez queira desabilitar essa opção. Os snapshots consistentes em caso de falha das workloads do SAP HANA não podem ser restaurados da mesma maneira.

9. Escolha Criar política padrão.

> **Note**
>
> Se receber um erro `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consulte Solução de problemas para obter mais informações.

AWS CLI

Para criar uma política de ciclo de vida de snapshots

Use o comando create-lifecycle-policy e inclua os parâmetros de `Scripts` em `CreateRule`. Para obter mais informações sobre os parâmetros, consulte Amazon Data Lifecycle Manager API Reference.

```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

Em que `policyDetails.json` inclui um dos seguintes itens dependendo do caso de uso:

- Backup do VSS

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "ExecutionHandler":"AWS_VSS_BACKUP",
                "ExecuteOperationOnScriptFailure":true|false,
```

```
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- Backup do SAP HANA

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- Documento do SSM personalizado

```
{
```

```
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

Considerações sobre os backups do VSS com o Amazon Data Lifecycle Manager

Com o Amazon Data Lifecycle Manager, você pode fazer backup e restaurar aplicações do Windows habilitadas para o VSS (Volume Shadow Copy Service) sendo executadas em instâncias do Amazon EC2. Se a aplicação tiver um gravador de VSS registrado no VSS do Windows, o Amazon Data Lifecycle Manager criará um snapshot que será consistente com a aplicação para essa aplicação.

> **Note**
>
> Atualmente, o Amazon Data Lifecycle Manager é compatível com snapshots consistentes com a aplicação apenas dos recursos executados no Amazon EC2, especificamente em cenários de backup em que os dados da aplicação podem ser restaurados substituindo uma instância existente por uma nova instância criada do backup. Nem todos os tipos de instância

ou aplicação são compatíveis com os backups do VSS. Para obter mais informações, consulte O que é AWS VSS? no Guia do usuário do Amazon EC2.

Tipos de instâncias não compatíveis

Os seguintes tipos de instância do Amazon EC2 não são compatíveis com backups do VSS. Se sua política tiver como alvo um desses tipos de instância, o Amazon Data Lifecycle Manager ainda poderá criar backups do VSS, mas os snapshots talvez não estejam marcados com as tags de sistema necessárias. Sem essas tags, os snapshots não serão gerenciados pelo Amazon Data Lifecycle Manager após sua criação. Pode ser necessário excluir esses snapshots manualmente.

- T3: `t3.nano` | `t3.micro`
- T3a: `t3a.nano` | `t3a.micro`
- T2: `t2.nano` | `t2.micro`

Responsabilidade compartilhada pelos snapshots consistentes com a aplicação

Você deve garantir que:

- O agente SSM está instalado e em execução nas instâncias de destino up-to-date
- O Systems Manager tenha permissões para executar as ações necessárias nas instâncias-alvo
- O Amazon Data Lifecycle Manager tenha permissões para realizar as ações do Systems Manager necessárias para executar scripts prévios e posteriores nas instâncias-alvo.
- Para cargas de trabalho personalizadas, como bancos de dados MySQL, PostgreSQL InterSystems ou IRIS autogerenciados, o documento SSM que você usa inclui as ações corretas e necessárias para congelar, limpar e descongelar a E/S da configuração do banco de dados.
- Os horários de criação de snapshots estejam alinhados com sua agenda de workload. Por exemplo, tente agendar a criação de snapshots durante as janelas de manutenção agendadas.

O Amazon Data Lifecycle Manager garante que:

- A criação do snapshot seja iniciada dentro de 60 minutos a partir do horário agendado para criação do snapshot.
- Os scripts prévios sejam executados antes do início da criação do snapshot.

- Os scripts posteriores sejam executados após o script prévio ser bem-sucedido e a criação do snapshot ter sido iniciada. O Amazon Data Lifecycle Manager só execute o script posterior se o script prévio for bem-sucedido. Se o script prévio falhar, o Amazon Data Lifecycle Manager não executará o script posterior.
- Os snapshots sejam marcados com as tags apropriadas na criação.
- CloudWatch métricas e eventos são emitidos quando os scripts são iniciados e quando falham ou são bem-sucedidos.

Outros casos de uso para scripts prévios e posteriores

Além de usar scripts prévios e posteriores para automatizar snapshots consistentes com a aplicação, você pode usar os scripts prévios e posteriores juntos ou individualmente para automatizar outras tarefas administrativas antes ou depois da criação do snapshot. Por exemplo: .

- Usar um script prévio para aplicar patches antes de criar os snapshots. Isso pode ajudar você a criar snapshots depois de aplicar as atualizações regulares de software semanais ou mensais.

> **Note**
>
> Se você escolher executar somente um script prévio, a opção Usar o padrão de snapshots consistentes em caso de falha será habilitada por padrão.

- Usar um script posterior para aplicar patches após a criação de snapshots. Isso pode ajudar você a criar snapshots antes de aplicar suas atualizações regulares de software semanais ou mensais.

Introdução a outros casos de uso

Esta seção explica as etapas que você precisa realizar ao usar scripts prévios e/ou scripts posteriores para outros casos de uso que não sejam de snapshots consistentes com a aplicação.

Etapa 1: preparar as instâncias-alvo

Para preparar as instâncias-alvo para scripts prévios e/ou posteriores

1. Instale o SSM Agent nas instâncias-alvo, se ainda não estiver instalado. Se o SSM Agent já estiver instalado em suas instâncias-alvo, pule esta etapa.

- (Instâncias do Linux) Instalar o SSM Agent manualmente em instâncias do Amazon EC2 para Linux
- (Instâncias do Windows) Instalar o SSM Agent manualmente em instâncias do Amazon EC2 para Windows

2. Certifique-se de que o SSM Agent esteja em execução. Para obter mais informações, consulte Verificar o status do SSM Agent e iniciar o agente.
3. Configure o Systems Manager para instâncias do Amazon EC2. Para obter mais informações, consulte Configuração do Systems Manager para instâncias Amazon EC2 no AWS Systems Manager Guia do usuário do .

Etapa 2: preparar o documento do SSM

Você deve criar um documento de comando do SSM que inclua os scripts prévios e/ou posteriores com os comandos que você deseja executar.

Você pode criar um documento do SSM usando o modelo de documento do SSM em branco abaixo e adicionar os comandos de script prévio e posterior nas seções apropriadas do documento.

⚠ Observe o seguinte:

- É sua responsabilidade garantir que o documento do SSM realize as ações corretas e necessárias para a sua workload.
- O documento do SSM deve incluir os campos obrigatórios para `allowedValues`, incluindo `pre-script`, `post-script` e `dry-run`. O Amazon Data Lifecycle Manager executará os comandos na instância com base no conteúdo dessas seções. Se o documento do SSM não tiver essas seções, o Amazon Data Lifecycle Manager o tratará como uma execução que falhou.

```
###============================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of this
# software and associated documentation files (the "Software"), to deal in the Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.
```

```
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###==============================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre and/
or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-
[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions during
 policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager to
 successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should be
 executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
```

```
 inputs:
   runCommand:
   - |
     #!/bin/bash


###==============================================================================###
     ### Error Codes

###==============================================================================###
     # The following Error codes will inform Data Lifecycle Manager of the type of
error
     # and help guide handling of the error.
     # The Error code will also be emitted via AWS Eventbridge events in the 'cause'
field.
     # 1 Pre-script failed during execution - 201
     # 2 Post-script failed during execution - 202
     # 3 Auto thaw occurred before post-script was initiated - 203
     # 4 Pre-script initiated while post-script was expected - 204
     # 5 Post-script initiated while pre-script was expected - 205
     # 6 Application not ready for pre or post-script initiation - 206


###==============================================================================###
     ### Global variables

###==============================================================================###
     START=$(date +%s)
     # For testing this script locally, replace the below with OPERATION=$1.
     OPERATION={{ command }}

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
     }

     # Add all post-script actions to be performed within the function below
     execute_post_script() {
         echo "INFO: Start execution of post-script"
     }

     # Debug logging for parameters passed to the SSM document
     echo "INFO: ${OPERATION} starting at $(date) with executionId: ${EXECUTION_ID}"
```

```
      # Based on the command parameter value execute the function that supports
      # pre-script/post-script operation
      case ${OPERATION} in
          pre-script)
              execute_pre_script
              ;;
          post-script)
              execute_post_script
              ;;
          dry-run)
              echo "INFO: dry-run option invoked - taking no action"
              ;;
          *)
              echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
              exit 1 # return failure
              ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

Etapa 3: preparar o perfil do IAM do Amazon Data Lifecycle Manager

> **Note**
>
> Essa etapa é necessária se:
>
> - Você criar ou atualizar uma política de snapshot habilitada para script prévio/posterior que usa um perfil do IAM personalizado.
> - Você usar a linha de comando para criar ou atualizar uma política de snapshot habilitado para script prévio/posterior.
>
> Se você usar o console para criar ou atualizar uma política de instantâneos ativada antes e depois do script que usa a função padrão para gerenciar snapshots () AWSDataLifecycleManagerDefaultRole, pule esta etapa. Nesse caso, anexamos automaticamente a AWSDataLifecycleManagerSSMFullAccesspolítica a essa função.

Você deve garantir que o perfil do IAM que você usa para a política conceda ao Amazon Data Lifecycle Manager permissão para realizar as ações do SSM necessárias para executar scripts prévios e posteriores nas instâncias-alvo da política.

O Amazon Data Lifecycle Manager fornece uma política gerenciada (AWSDataLifecycleManagerSSMFullAccess) que inclui as permissões necessárias. Você pode anexar essa política ao perfil do IAM para gerenciar snapshots e garantir que ela inclua as permissões.

> **Important**
>
> A política AWSDataLifecycleManagerSSMFullAccess gerenciada usa a chave de `aws:ResourceTag` condição para restringir o acesso a documentos SSM específicos ao usar scripts anteriores e posteriores. Para permitir que o Amazon Data Lifecycle Manager acesse os documentos do SSM, você deve garantir que eles estejam marcados com `DLMScriptsAccess:true`.

Ou então, você pode criar manualmente uma política personalizada ou atribuir as permissões necessárias diretamente ao perfil do IAM que você usa. Você pode usar as mesmas permissões definidas na política AWSDataLifecycleManagerSSMFullAccess gerenciada, no entanto, a chave de `aws:ResourceTag` condição é opcional. Se você decidir não usar essa chave de condição, não precisará marcar os documentos do SSM com `DLMScriptsAccess:true`.

Use um dos métodos a seguir para adicionar a AWSDataLifecycleManagerSSMFullAccesspolítica à sua função do IAM.

Console

Para anexar a política gerenciada ao seu perfil personalizado

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Roles (Funções).
3. Pesquise e selecione o perfil personalizado para gerenciar os snapshots.
4. Na guia Permissões, escolha Adicionar permissões, Anexar políticas.
5. Pesquise e selecione a política AWSDataLifecycleManagerSSMFullAccessgerenciada e, em seguida, escolha Adicionar permissões.

AWS CLI

Para anexar a política gerenciada ao seu perfil personalizado

Use o comando attach-role-policy. Para `---role-name`, especifique o nome do seu perfil personalizado. Em `--policy-arn`, especifique `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`.

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Criar uma política de ciclo de vida de snapshots

Console

Para criar uma política de ciclo de vida de snapshots

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Na tela Select policy type (Selecionar tipo de política), escolha EBS snapshot policy (Política de snapshot do EBS) e depois Next (Próximo).
4. Na seção Target resources (Recursos de destino), faça o seguinte:
   a. Para Tipos de recursos-alvo, escolha `Instance`.
   b. Para Tags de recurso-alvo, especifique as tags de recurso que identificam as instâncias para backup. Só será feito backup dos recursos que têm as tags especificadas.
5. Para a função do IAM, escolha AWSDataLifecycleManagerDefaultRole(a função padrão para gerenciar instantâneos) ou escolha uma função personalizada que você criou e preparou para scripts anteriores e posteriores.
6. Configure as agendas e as opções adicionais conforme necessário. Recomendamos que você agende a criação dos snapshots para períodos que atendam à sua workload, como durante janelas de manutenção.
7. Na seção Scripts prévios e posteriores, selecione Habilitar scripts prévios e posteriores e depois faça o seguinte:

a. Selecione Documento do SSM personalizado.

b. Para Opção de automatização, escolha a opção que corresponde aos scripts que você deseja executar.

c. Para Documento do SSM, selecione o documento do SSM que você preparou.

8. Configure as seguintes opções adicionais se necessário:

- Tempo limite do script: o período limite após o qual o Amazon Data Lifecycle Manager considera que a tentativa de execução do script falhou se ela não foi concluída. Se um script não for concluído dentro do período limite, o Amazon Data Lifecycle Manager considerará que a tentativa falhou. O período de tempo limite se aplica aos scripts prévios e posteriores individualmente. O limite de tempo mínimo e padrão é de 10 segundos. E o tempo limite máximo é de 120 segundos.
- Tentar os scripts com falha novamente: selecione essa opção para fazer novas tentativas de executar os scripts que não forem concluídos dentro do período de tempo limite. Se o script prévio falhar, o Amazon Data Lifecycle Manager tentará realizar novamente todo o processo de criação de snapshots, incluindo a execução dos scripts prévios e posteriores. Se o script posterior falhar, o Amazon Data Lifecycle Manager fará nova tentativa de executar apenas o script posterior; nesse caso, o script prévio estará sido concluído e o snapshot poderá ter sido criado.
- Usar o padrão de snapshots consistentes em caso de falha: selecione essa opção para usar padrão de snapshots consistentes em caso de falha se a execução do script prévio falhar. Esse é o comportamento padrão da criação de snapshots para o Amazon Data Lifecycle Manager se os scripts prévios e posteriores não estiverem habilitados. Se você habilitou novas tentativas, o Amazon Data Lifecycle Manager só usará o padrão de snapshots consistentes em caso de falha após esgotar o todas as tentativas. Se o script prévio falhar e você não usar o padrão de snapshots consistentes em caso de falha, o Amazon Data Lifecycle Manager não criará snapshots para a instância durante da execução agendada.

9. Escolha Criar política padrão.

> **Note**
>
> Se receber um erro `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consulte Solução de problemas para obter mais informações.

AWS CLI

Para criar uma política de ciclo de vida de snapshots

Use o comando create-lifecycle-policy e inclua os parâmetros de `Scripts` em `CreateRule`. Para obter mais informações sobre os parâmetros, consulte Amazon Data Lifecycle Manager API Reference.

```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

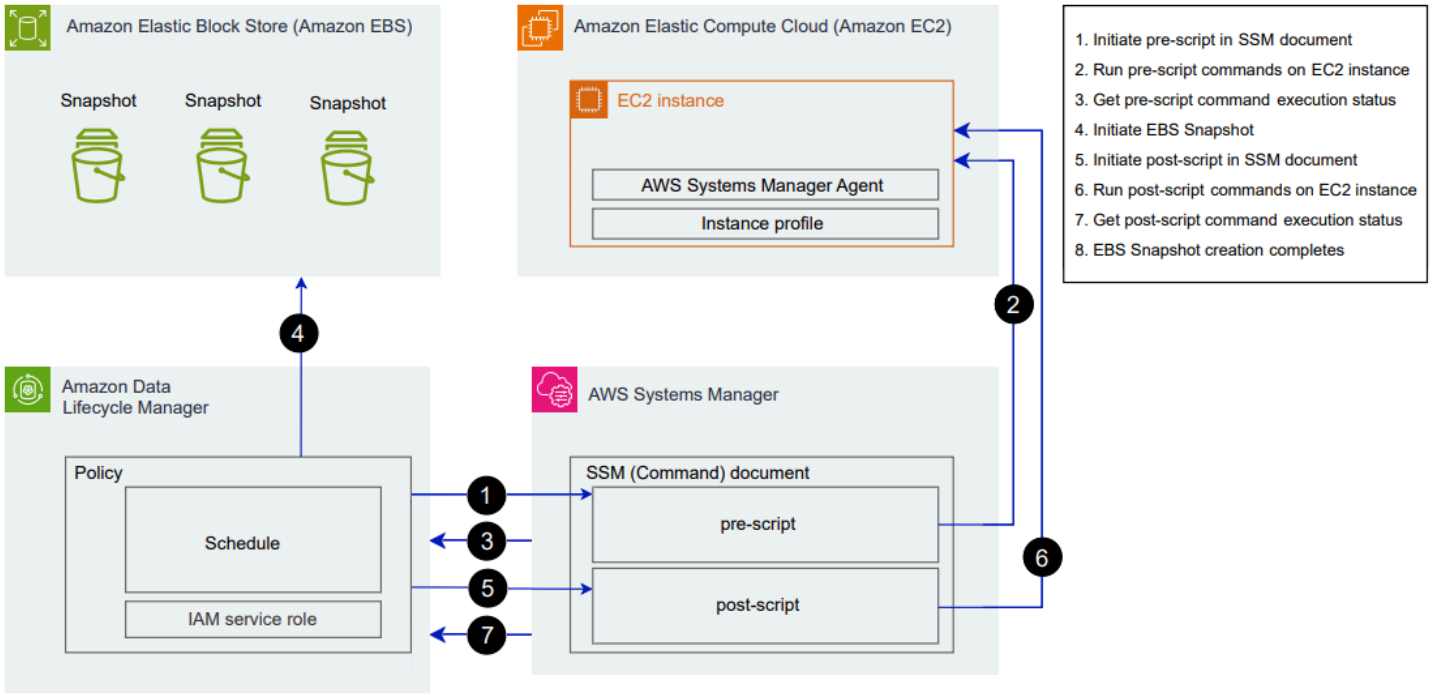
Em que `policyDetails.json` inclui o seguinte:

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE" | "POST" | "PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
```

```
}
```

Como funcionam os scripts prévios e posteriores

A imagem a seguir mostra o fluxograma dos scripts prévios e posteriores ao usar documentos do SSM personalizados. Isso não se aplica aos backups do VSS.



No horário agendado para a criação dos snapshots, as seguintes ações e interações entre serviços ocorrem.

1. O Amazon Data Lifecycle Manager inicia a ação de script prévio chamando o documento do SSM e passando o parâmetro `pre-script`.

   > **Note**
   >
   > As etapas 1 a 3 só ocorrem se você executar os scripts prévios. Se você executar somente os scripts posteriores, as etapas 1 a 3 serão ignoradas.

2. O Systems Manager envia os comandos do script prévio para o SSM Agent em execução nas instâncias-alvo. O SSM Agent executa os comandos na instância e envia as informações de status de volta ao Systems Manager.

Por exemplo, se o documento do SSM for usado para criar snapshots consistentes com a aplicação, o script prévio poderá congelar e descarregar a E/S para garantir que todos os dados armazenados em buffer sejam gravados no volume antes que o snapshot seja feito.

3. O Systems Manager envia atualizações de status dos comandos do script prévio para o Amazon Data Lifecycle Manager. Se o script prévio falhar, o Amazon Data Lifecycle Manager fará uma das seguintes ações, dependendo de como você configurar as opções de script prévio e posterior:

Repetições	Usar o padrão de snapshots consistentes em caso de falha	Ação
Habilitado com novas tentativas restantes	Habilitado	Fazer novas tentativas de executar o script até que ele seja bem-sucedido ou que as novas tentativas sejam esgotadas
Esgotadas sem conclusão bem-sucedida	Habilitado	Criar snapshots consistentes em caso de falha e não executar o script posterior.
Habilitado com novas tentativas restantes	Desabilitado	Fazer novas tentativas de executar o script até que ele seja bem-sucedido ou que as novas tentativas sejam esgotadas
Esgotadas sem conclusão bem-sucedida	Desabilitado	Ignorar a criação do snapshot para a instância-alvo e não executar o script posterior.
Desabilitado	Habilitado	Criar snapshots consistentes em caso de falha e não executar o script posterior.
Desabilitado	Desabilitado	Ignorar a criação do snapshot para a instância-alvo e não executar o script posterior.

4. O Amazon Data Lifecycle Manager inicia a criação de snapshots.
5. O Amazon Data Lifecycle Manager inicia a ação do script posterior chamando o documento do SSM e passando o parâmetro `post-script`.

> **Note**
>
> As etapas 5 a 7 só ocorrem se você executar os scripts prévios. Se você executar somente os scripts posteriores, as etapas 1 a 3 serão ignoradas.

6. O Systems Manager envia os comandos do script posterior para o SSM Agent em execução nas instâncias-alvo. O SSM Agent executa os comandos na instância e envia as informações de status de volta ao Systems Manager.

   Por exemplo, se o documento do SSM permitir snapshots consistentes com a aplicação, esse script posterior poderá descongelar a E/S para garantir que seus bancos de dados retomem as operações normais de E/S após o snapshot ser feito.
7. Se você executar um script posterior e o Systems Manager indicar que ele foi concluído com sucesso, o processo será concluído.

   Se o script posterior falhar, o Amazon Data Lifecycle Manager fará uma das seguintes ações, dependendo de como você configurar as opções de script prévio e posterior:

Repetições	Ação
Habilitado com novas tentativas restantes	Repita o script posterior até que ele seja bem-sucedido ou que as novas tentativas sejam esgotadas
Esgotado sem sucesso	Ignorar script posterior
Desabilitado	Ignorar script posterior

Lembre-se de que, se o script posterior falhar, o script prévio (se habilitado) será concluído com sucesso e os snapshots poderão ter sido criados. Talvez seja necessário realizar outras ações na instância para garantir que ela esteja operando como esperado. Por exemplo, se o script prévio pausou e descarregou a E/S, mas o script posterior falhou ao descongelar a E/S, talvez seja necessário configurar o banco de dados para descongelar automaticamente a E/S ou que você precise descongelar a E/S manualmente.

8. O processo de criação do snapshot talvez seja concluído após a conclusão do script posterior. O tempo necessário para concluir o snapshot depende do tamanho do snapshot.

Identificar os snapshots criados com scripts prévios e posteriores

O Amazon Data Lifecycle Manager atribui automaticamente as seguintes tags do sistema aos snapshots criados com scripts prévios e posteriores.

- Chave: `aws:dlm:pre-script`; valor: `SUCCESS|FAILED`

  Um valor de tag de `SUCCESS` indica que o script prévio foi executado com sucesso. Um valor de tag de `FAILED` indica que o script prévio não foi executado com sucesso.
- Chave: `aws:dlm:post-script`; valor: `SUCCESS|FAILED`

  Um valor de tag de `SUCCESS` indica que o script posterior foi executado com sucesso. Um valor de tag de `FAILED` indica que o script posterior não foi executado com sucesso.

Para documentos do SSM personalizados e backups do SAP HANA, você pode inferir a criação bem-sucedida de snapshots consistentes com a aplicação se o snapshot estiver marcado com `aws:dlm:pre-script:SUCCESS` e `aws:dlm:post-script:SUCCESS`.

Além disso, snapshots consistentes com a aplicação criados usando o backup do VSS são automaticamente marcados com:

- Chave: `AppConsistent tag`; valor: `true|false`

  Um valor de tag de `true` indica que o backup do VSS foi bem-sucedido e que os snapshots são consistentes com a aplicação. Um valor de tag de `false` indica que o backup do VSS não foi bem-sucedido e que os snapshots não são consistentes com a aplicação.

Monitorar a execução do script prévio e posterior

CloudWatch Métricas da Amazon

O Amazon Data Lifecycle Manager publica as seguintes CloudWatch métricas quando os scripts anteriores e posteriores falham e são bem-sucedidos e quando os backups do VSS falham e são bem-sucedidos.

- `PreScriptStarted`

- `PreScriptCompleted`
- `PreScriptFailed`
- `PostScriptStarted`
- `PostScriptCompleted`
- `PostScriptFailed`
- `VSSBackupStarted`
- `VSSBackupCompleted`
- `VSSBackupFailed`

Para ter mais informações, consulte Monitore suas políticas usando a Amazon CloudWatch.

Amazon EventBridge

O Amazon Data Lifecycle Manager emite o seguinte evento da EventBridge Amazon quando um script pré ou pós-script é iniciado, é bem-sucedido ou falha

- `DLM Pre Post Script Notification`

Para ter mais informações, consulte Monitore suas políticas usando CloudWatch Eventos.

Automatizar ciclos de vida da AMI

O procedimento a seguir mostra como usar o Amazon Data Lifecycle Manager para automatizar os ciclos de vida da AMI com suporte do EBS.

Tópicos

Criar uma política de ciclo de vida de AMI

Use os procedimentos a seguir para criar uma política de ciclo de vida de AMI.

Console

Para criar uma política de AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Na tela Select policy type (Selecionar tipo de política), escolha EBS-backed AMI policy (Política de AMI com suporte do EBS) e depois Next (Próximo).
4. Na seção Target resources (Recursos de destino), em Target resource tags (Etiquetas de recurso de destino), escolha as etiquetas de recursos que identificam os volumes ou as instâncias dos quais deseja fazer backup. A política só oferece suporte aos recursos que tenham a chave de etiqueta e os pares de valor especificados.
5. Para Description (Descrição), insira uma breve descrição da rota.
6. Em IAM role (Função do IAM), selecione a função do IAM que tem permissões para gerenciar AMIs e snapshots e para descrever instâncias. Para usar a função padrão fornecida pelo Amazon Data Lifecycle Manager, escolha Default role (Função padrão). Se preferir, para usar uma função do IAM personalizada criada anteriormente, selecione Choose another role (Escolher outra função) e selecione a função a ser usada.
7. Em Policy tags (Etiquetas de políticas), adicione as etiquetas a serem aplicadas na política de ciclo de vida. É possível usar essas etiquetas para identificar e categorizar suas políticas.
8. Em Policy status after creation (Status da política após a criação), selecione Enable policy (Habilitar política) para iniciar as execuções da política no próximo horário agendado ou Disable policy (Desabilitar política) para impedir que a política seja executada. Se você não habilitar a política agora, ela não começará a criar AMIs até que você a ative manualmente após a criação.
9. Na seção Instance reboot (Reinicialização da instância), indique se as instâncias devem ser reinicializadas antes da criação da AMI. Para evitar que as instâncias de destino sejam reinicializadas, escolha No (Não). Escolher No (Não) pode causar problemas de consistência de dados. Para reiniciar instâncias antes da criação da AMI, escolhaYes (Sim). Escolher isso garante a consistência dos dados, mas pode resultar na reinicialização de várias instâncias direcionadas simultaneamente.
10. Selecione Next (Próximo).
11. Em Configure schedule (Configurar agendamento), configure os agendamentos de política. Uma política pode ter até quatro agendamentos. A Programação 1 é obrigatória.

As Programações 2, 3 e 4 são opcionais. Para cada agendamento de política que você adicionar, faça o seguinte:

a. Na seção Schedule details (Detalhes do agendamento), faça o seguinte:

   i. Em Schedule name (Nome do agendamento), especifique um nome descritivo para o agendamento.

   ii. Em Frequency (Frequência) e nos campos relacionados, configure o intervalo entre as execuções da política.

      É possível configurar execuções de políticas com uma programação diária, semanal, mensal ou anual. Como opção, escolha Custom cron expression (Expressão cron personalizada) para especificar um intervalo de até 1 ano. Para obter mais informações, consulte Expressões Cron no Guia do usuário do Amazon CloudWatch Events.

   iii. Em Starting at (Iniciando às), especifique a hora para iniciar as execuções da política. A primeira execução da política inicia uma hora depois do horário agendado. É necessário inserir a hora no formato `hh:mm` UTC.

   iv. Em Retention type (Tipo de retenção), especifique a política de retenção para AMIs criadas pelo agendamento.

      É possível reter AMIs com base na contagem total ou na idade delas.

      Para retenção baseada em contagem, o intervalo é de `1` a `1000`. Quando a contagem máxima for atingida, a AMI mais antiga será excluída quando uma nova for criada.

      Para retenção baseada na idade, o intervalo é de `1` dia a `100` anos. Depois que o período de retenção de cada AMI expirar, ela será excluída.

      > **Note**
      >
      > Todas as programações devem ter o mesmo tipo de retenção. É possível especificar o tipo de retenção somente para a Programação 1. As Programações 2, 3 e 4 herdam o tipo de retenção da Programação 1. Cada programação pode ter sua própria contagem ou período de retenção.

b. Configurar a marcação para AMIs.

Na seção Tagging (Marcação), faça o seguinte:

i. Para copiar todas as etiquetas definidas por usuário da instância de origem para as AMIs criadas pelo agendamento, selecione Copy tags from source (Copiar etiquetas da origem).

ii. Por padrão, as AMIs criadas pelo agendamento são automaticamente marcadas com o ID da instância de origem. Para evitar que essa marcação automática ocorra, em Variable tags (Etiquetas de variáveis), remova o bloco `instance-id: $(instance-id)`.

iii. Para especificar etiquetas adicionais a serem atribuídas às AMIs criadas por esse agendamento, escolha Add tags (Adicionar etiquetas).

c. Configurar a suspensão de uso da AMI.

Para defasar as AMIs quando elas não devem mais ser usadas, na seção Defasagem da AMI, selecione Habilitar a defasagem da AMI para esta programação e, em seguida, especifique a regra de defasagem da AMI. A regra de defasagem da AMI especifica quando as AMIs devem ser defasadas.

Se a programação usar retenção de AMI baseada em contagem, será necessário especificar o número de AMIs mais antigas a serem defasadas. A contagem de defasagem deve ser menor ou igual à contagem de retenção de AMI da programação e não pode ser maior que 1.000. Por exemplo, se a programação estiver configurada para reter no máximo 5 AMIs, será possível configurar a programação para defasar até 5 das AMIs mais antigas.

Se a programação usar retenção de AMI baseada em idade, será necessário especificar o período após o qual as AMIs serão defasadas. A contagem de defasagem deve ser menor ou igual ao período de retenção da AMI da programação e não pode ser superior a 10 anos (120 meses, 520 semanas ou 3.650 dias). Por exemplo, se a programação estiver configurada para reter AMIs por 10 dias, será possível configurar a programação para substituir AMIs após períodos de até 10 dias após a criação.

d. Configurar cópia entre regiões.

Para copiar AMIs criadas pelo agendamento para regiões diferentes, na seção Cross-Region copy (Cópia entre regiões), selecione Enable cross-Region copy (Habilitar cópia entre regiões). É possível copiar AMIs para até três regiões adicionais em sua conta. Especifique uma regra de cópia entre regiões separada para cada região de destino.

Para cada região de destino, é possível especificar o seguinte:

- Uma política de retenção para a cópia AMI. Quando o período de retenção expirar, a cópia na região de destino será automaticamente cancelada.
- Status de criptografia para a cópia da AMI. Se a AMI de origem estiver criptografada ou se a criptografia por padrão estiver habilitada, as AMIs copiadas serão sempre criptografadas. Se a AMI de origem não estiver criptografada e a criptografia por padrão estiver desabilitada, será possível habilitar a criptografia. Se você não especificar uma chave do KMS, as AMIs serão criptografadas usando a chave do KMS padrão de criptografia do EBS em cada região de destino. Se você especificar uma Chave do KMS para a região de destino, a função do IAM selecionada deverá ter acesso à Chave do KMS.
- Uma regra de defasagem para a cópia da AMI. Quando o período de descontinuação expira, a cópia da AMI é automaticamente substituída. O período de defasagem deve ser menor ou igual ao período de retenção de cópias e não pode ser superior a 10 anos.
- Se deseja copiar todas as marcações ou nenhuma marcação da AMI de origem.

> **Note**
>
> Não exceda o número de cópias de AMI simultâneas por região.

e. Para adicionar outros agendamentos, escolha Add another schedule (Adicionar outro agendamento), localizado na parte superior da tela. Para cada agendamento adicional, preencha os campos conforme descrito anteriormente neste tópico.

f. Depois de adicionar os agendamentos necessárias, escolha Review policy (Revisar política).

12. Revise o resumo da política e escolha Create policy (Criar política).

> **Note**
>
> Se receber um erro `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists`, consulte Solução de problemas para obter mais informações.

Command line

Use o comando create-lifecycle-policy para criar uma política de ciclo de vida de AMI. Para `PolicyType`, especifique `IMAGE_MANAGEMENT`.

> **Note**
>
> Para simplificar a sintaxe, os exemplos a seguir usam um arquivo JSON `policyDetails.json`, que inclui os detalhes da política.

Exemplo 1: retenção baseada em idade e defasagem de AMI

Esse exemplo cria uma política de ciclo de vida da AMI que cria AMIs de todas as instâncias que têm uma chave de marcação `purpose` com um valor de `production` e reinicializa as instâncias direcionadas. A política inclui uma programação que cria uma AMI todos os dias às `01:00` UTC. A política mantém AMIs por 2 dias e faz a defasagem depois de 1 dia. Também copia as etiquetas da instância de origem para as AMIs criadas por ela.

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "purpose",
        "Value": "production"
    }],
    "Schedules": [{
            "Name": "DailyAMIs",
            "TagsToAdd": [{
                "Key": "type",
```

```
                "Value": "myDailyAMI"
            }],
            "CreateRule": {
                "Interval": 24,
                "IntervalUnit": "HOURS",
                "Times": [
                    "01:00"
                ]
            },
            RetainRule":{
                "Interval" : 2,
                "IntervalUnit" : "DAYS"
            },
            DeprecateRule": {
                "Interval" : 1,
                "IntervalUnit" : "DAYS"
            },
            "CopyTags": true
        }
    ],
    "Parameters" : {
        "NoReboot":true
    }
}
```

Se a solicitação for bem-sucedida, o comando retornará o ID da política recém-criada. O seguinte é um exemplo de saída.

```
{
   "PolicyId": "policy-9876543210abcdef0"
}
```

Exemplo 2: retenção baseada em contagem e defasagem de AMI com cópia entre regiões

Esse exemplo cria uma política de ciclo de vida da AMI que cria AMIs de todas as instâncias que têm uma chave de marcação `purpose` com um valor de `production` e reinicializa as instâncias direcionadas. A política inclui uma programação que cria uma AMI a cada 6 horas a partir de `17:30` UTC. A política retém AMIs `3` e faz a defasagem automaticamente de `2` AMIs mais antigas. Ela também tem uma regra de cópia entre regiões que copia AMIs para `us-east-1`, mantém 2 cópias de AMI e faz a defasagem automaticamente da AMI mais antiga.

```
aws dlm create-lifecycle-policy \
```

```
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes" : [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key":"purpose",
        "Value":"production"
    }],
    "Parameters" : {
          "NoReboot": true
    },
    "Schedules" : [{
        "Name" : "Schedule1",
        "CopyTags": true,
        "CreateRule" : {
            "Interval": 6,
            "IntervalUnit": "HOURS",
            "Times" : ["17:30"]
        },
        "RetainRule":{
            "Count" : 3
        },
        "DeprecateRule":{
            "Count" : 2
        },
        "CrossRegionCopyRules": [{
            "TargetRegion": "us-east-1",
            "Encrypted": true,
            "RetainRule":{
                "IntervalUnit": "DAYS",
                "Interval": 2
            },
            "DeprecateRule":{
                "IntervalUnit": "DAYS",
```

```
                "Interval": 1
            },
            "CopyTags": true
        }]
    }]
}
```

Considerações sobre políticas de ciclo de vida da AMI

As seguintes considerações gerais se aplicam à criação de políticas de ciclo de vida de AMIs:

- As políticas de ciclo de vida da AMI visam somente instâncias que estão na mesma região que a política.
- A primeira operação de criação de AMI começa uma hora após o horário de início especificado. As operações de criação de AMI subsequentes começam uma hora após o horário programado.
- Quando o Amazon Data Lifecycle Manager cancela o registro de uma AMI, ele exclui automaticamente o backup de snapshots.
- Tags de recursos de destino diferenciam letras maiúsculas de minúsculas.
- Se você remover as tags de destino de uma instância visada por uma política, o Amazon Data Lifecycle Manager não gerenciará mais os AMIs existentes no padrão, você deverá excluí-los manualmente se eles não forem mais necessários.
- É possível criar várias políticas para fazer backup de uma instância. Por exemplo, se uma instância tiver 2 etiquetas, com a etiqueta A como o destino da política A para criar uma AMI a cada 12 horas, e a etiqueta B como o destino da política B para criar uma AMI a cada 24 horas, o Amazon Data Lifecycle Manager cria AMIs de acordo com as programações de ambas as políticas. Como alternativa, é possível obter o mesmo resultado criando uma única política que tenha várias programações. Por exemplo, é possível criar uma única política voltada apenas para tag A e especificar duas programações: uma para cada 12 horas e uma para cada 24 horas.
- Novos volumes associados a uma instância de destino após a criação da política são incluídos automaticamente no backup na próxima execução da política. Todos os volumes associados à instância no momento da execução da política são incluídos.
- Se você criar uma política com uma programação personalizada baseada em cron que esteja configurada para criar apenas uma AMI, a política não cancelará automaticamente o registro dessa AMI quando o limite de retenção for atingido. É necessário cancelar manualmente o registro da AMI caso ela não seja mais necessária.

- Se você criar uma política baseada na idade em que o período de retenção seja menor do que a frequência de criação, o Amazon Data Lifecycle Manager sempre reterá o última AMI até que a próxima seja criada. Por exemplo, se uma política baseada na idade criar uma AMI por mês com um período de retenção de sete dias, o Amazon Data Lifecycle Manager reterá cada AMI por um mês, mesmo que o período de retenção seja de sete dias.
- Para políticas baseadas em contagem, o Amazon Data Lifecycle Manager sempre cria AMIs de acordo com a frequência de criação antes de tentar cancelar o registro da AMI mais antiga de acordo com a política de retenção.
- Pode levar várias horas para cancelar com êxito o registro de uma AMI e excluir os snapshots de backup associados. Se o Amazon Data Lifecycle Manager criar a próxima AMI antes que a AMI criada anteriormente seja cancelada com êxito, você poderá reter temporariamente um número de AMIs que maior do que sua contagem de retenção.

Os seguintes fatores são aplicáveis ao encerramento de instâncias direcionado por uma política:

- Se você encerrar uma instância que foi direcionada por uma política com uma programação de retenção baseada em contagem, a política deixará de gerenciar as AMIs que criou anteriormente com base na instância encerrada. É necessário cancelar manualmente o registro dessas AMIs mais antigas caso elas não sejam mais necessárias.
- Se você encerrar uma instância que foi direcionada por uma política com uma programação de retenção baseada em idade, a política continuará a cancelar registros de AMIs que foram criadas anteriormente com base na instância encerrada de acordo com a programação definida até a última AMI (mas sem incluí-la). É necessário cancelar manualmente o registro da última AMI caso ela não seja mais necessária.

As considerações a seguir se aplicam às políticas de AMI à descontinuação de AMIs:

- Se você aumentar a contagem de defasagem da AMI para uma programação com retenção baseada em contagem, a alteração será aplicada a todas as AMIs (atuais e novas) criadas pela programação.
- Se você aumentar o período de defasagem da AMI para uma programação com retenção baseada em idade, a alteração será aplicada somente a novas AMIs. AMIs atuais não são afetadas.
- Se você remover a regra de defasagem da AMI de uma programação, o Amazon Data Lifecycle Manager não cancelará a defasagem de AMIs que foram anteriormente consideradas defasadas por essa programação.

- Se você diminuir a contagem ou período de defasagem da AMI de uma programação, o Amazon Data Lifecycle Manager não cancelará a defasagem de AMIs que foram anteriormente consideradas defasadas por essa programação.
- Se você defasar manualmente uma AMI criada por uma política de AMI, o Amazon Data Lifecycle Manager não substituirá a defasagem.
- Se você cancelar manualmente a defasagem de uma AMI que foi anteriormente defasada por uma política de AMI, o Amazon Data Lifecycle Manager não substituirá o cancelamento.
- Se uma AMI for criada por várias programações conflitantes e uma ou mais dessas programações não tiverem uma regra de defasagem da AMI, o Amazon Data Lifecycle Manager não vai defasar essa AMI.
- Se uma AMI for criada por várias programações conflitantes e todas essas programações tiverem uma regra de descontinuação da AMI, o Amazon Data Lifecycle Manager usará a regra de descontinuação que resulte na data de descontinuação mais posterior.

As seguintes considerações se aplicam a políticas de AMI e à Lixeira:

- Se o Amazon Data Lifecycle Manager cancelar o registro de uma AMI e enviá-la para a lixeira quando o limite de retenção da política for atingido e você restaurar manualmente essa AMI da lixeira, você deverá cancelar manualmente o registro dessa AMI quando ela não for mais necessária. O Amazon Data Lifecycle Manager não poderá mais gerenciar a AMI.
- Se você cancelar manualmente o registro uma AMI criada por uma política e essa AMI estiver na lixeira quando o limite de retenção da política for atingido, o Amazon Data Lifecycle Manager não cancelará o registro da AMI. O Amazon Data Lifecycle Manager não gerencia AMIs enquanto elas estão na lixeira.

  Se a AMI for restaurada da lixeira antes que o limite de retenção da política seja atingido, o Amazon Data Lifecycle Manager cancelará o registro da AMI quando o limite de retenção da política for atingido.

  Se a AMI for restaurada da lixeira depois que o limite de retenção da política seja atingido, o Amazon Data Lifecycle Manager não canelará mais o registro da AMI. Exclua-a manualmente quando ela não for mais necessária.

As seguintes considerações se aplicam a políticas de AMI que estão no estado error:

- Para políticas com programações de retenção com base na idade, as AMIs configuradas para expirar enquanto a política estiver no estado `error` serão retidas por tempo indeterminado. É necessário cancelar o registro das AMIs manualmente. Quando você habilita a política novamente, o Amazon Data Lifecycle Manager retoma o cancelamento de registro de snapshots à medida que seus períodos de retenção expiram.
- Para políticas com programas de retenção com base em contagem, a política interrompe a criação e o cancelamento de registro de AMIs enquanto está no estado `error`. Ao reabilitar a política, o Amazon Data Lifecycle Manager retoma a criação de AMIs e retoma o cancelamento de registro de AMIs quando o limite de retenção é atingido.

As considerações a seguir se aplicam às políticas de AMI e à desativação de AMIs:

- Se você desabilitar uma AMI criada pelo Amazon Data Lifecycle Manager, e essa AMI for desabilitada quando o limite de retenção for atingido, o Amazon Data Lifecycle Manager cancelará o registro da AMI e excluirá seus snapshots associados.
- Se você desabilitar uma AMI criada pelo Amazon Data Lifecycle Manager e arquivar manualmente seus snapshots associados, e esses snapshots forem arquivados quando seu limite de retenção for atingido, o Amazon Data Lifecycle Manager não excluirá esses snapshots e não os gerenciará mais.

A consideração a seguir se aplica às políticas da AMI e à proteção de cancelamento de registro da AMI:

- Se você ativar manualmente a proteção de cancelamento de registro para uma AMI criada pelo Amazon Data Lifecycle Manager e ela ainda estiver ativada quando o limite de retenção da AMI for atingido, o Amazon Data Lifecycle Manager não gerenciará mais essa AMI. Você deve cancelar manualmente o registro da AMI e excluir seus snapshots subjacentes se ela não for mais necessária.

Recursos adicionais do

Para obter mais informações, consulte o blog Automatizando o snapshot e o gerenciamento de AMI do Amazon EBS usando o Amazon AWS Data Lifecycle Manager.

Automatizar cópias de snapshots entre contas

A automatização de cópias de snapshots entre contas permite copiar seus snapshots do Amazon EBS para regiões específicas em uma conta isolada e criptografar esses snapshots com uma chave de criptografia. Isso permite que você se proteja contra perda de dados no caso de sua conta ser comprometida.

A automatização de cópias de snapshots entre contas envolve duas contas:

- Conta de origem—A conta de origem é a conta que cria e compartilha os snapshots com a conta de destino. Nessa conta, você deve criar uma política de instantâneos do EBS que crie instantâneos em intervalos definidos e depois os compartilhe com outras contas. AWS
- Contade destino—A conta de destino é a conta com a conta de destino com a qual os snapshots são compartilhados e é a conta que cria cópias dos instantâneos compartilhados. Nesta conta, crie uma política de eventos de cópia entre contas que copia automaticamente snapshots compartilhados com ela por uma ou mais contas de origem especificadas.

Tópicos

Criar políticas de cópia de snapshot entre contas

Para preparar as contas de origem e de destino para cópia de snapshot entre contas, você precisa executar as seguintes etapas:

Etapa 1: Criar a política de snapshot do EBS (conta de origem)

Na conta de origem, crie uma política de snapshot do EBS que criará os snapshots e os compartilhará com as contas de destino necessárias.

Ao criar a política, certifique-se de habilitar o compartilhamento entre contas e de especificar as AWS contas de destino com as quais compartilhar os instantâneos. Estas são as contas com as quais os snapshots devem ser compartilhados. Se você estiver compartilhando snapshots criptografados, deverá dar permissão às contas de destino selecionadas para usar a Chave do KMS usada para

criptografar o volume de origem. Para ter mais informações, consulte Etapa 2: Compartilhe a chave gerenciada pelo cliente (Conta de origem).

> **Note**
>
> Você só pode compartilhar snapshots não criptografados ou criptografados usando uma chave gerenciada pelo cliente gerenciada pelo cliente. Você não pode compartilhar snapshots criptografados com a Chave do KMS de criptografia padrão do EBS. Se você compartilhar snapshots criptografados, também deverá compartilhar a Chave do KMS usada para criptografar o volume de origem com as contas de destino. Para obter mais informações, consulte Como permitir que usuários em outras contas usem uma chave do KMS no Guia do desenvolvedor do AWS Key Management Service .

Para obter mais informações sobre como criar um snapshot de política do EBS, consulte Automação dos ciclos de vida do snapshot.

Use um dos métodos a seguir para criar a política de snapshot do EBS.

Etapa 2: Compartilhe a chave gerenciada pelo cliente (Conta de origem)

Se você estiver compartilhando snapshots criptografados, conceda a função do IAM e as contas da AWS de destino (que você selecionou na etapa anterior) permissões para usar a chave gerenciada pelo cliente que foi usada para criptografar o volume de origem.

> **Note**
>
> Execute esta etapa apenas se você estiver compartilhando snapshots criptografados. Se você estiver compartilhando snapshots não criptografados, pule esta etapa.

Console

1. Abra o AWS KMS console em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Customer managed key (Chave gerenciadas pelo cliente) e selecione a chave do KMS que você precisa compartilhar com as contas de destino.

Anote o ARN das Chave do KMS, você precisará disso mais tarde.

4. Na guia Key policy (Política de chaves), role para baixo até a seção Key users (Usuários chave). Escolha Add (Adicionar), insira o nome da função do IAM que você selecionou na etapa anterior e escolha Add (Adicionar).
5. Na guia Key policy (Política de chaves), role para a seção Other AWS accounts (Outras contas da). Escolha Adicionar outras AWS contas e, em seguida, adicione todas as AWS contas de destino com as quais você escolheu compartilhar os instantâneos na etapa anterior.
6. Selecione Save changes (Salvar alterações).

Command line

Use o comando get-key-policy para recuperar a política de chaves que está atualmente vinculada à Chave do KMS.

Por exemplo, o comando a seguir recupera a política de chaves para uma Chave do KMS com um ID de `9d5e2b3d-e410-4a27-a958-19e220d83a1e` e a grava em um arquivo chamado `snapshotKey.json`.

```
$ aws kms get-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --query Policy \
    --output text > snapshotKey.json
```

Abra a política de chaves usando seu editor de texto preferido. Adicione o ARN da função do IAM que você especificou quando criou a política de snapshot e os ARNs das contas de destino com as quais deseja compartilhar a Chave do KMS.

Por exemplo, na política a seguir, adicionamos o ARN da função padrão do IAM e o ARN da conta raiz da conta de destino `222222222222`.

> **Tip**
>
> Para seguir o princípio de menor privilégio, não permita acesso total a `kms:CreateGrant`. Em vez disso, use a chave de `kms:GrantIsForAWSResource` condição para permitir que o usuário crie concessões na chave KMS somente quando a

concessão for criada em nome do usuário por um AWS serviço, conforme mostrado no exemplo a seguir.

```
{
    "Sid" : "Allow use of the key",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Allow attachment of persistent resources",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource" : "*",
    "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
```

```
    }
}
```

Salve e feche o arquivo . Use então o comando put-key-policy para anexar a política chave atualizada à Chave do KMS.

```
$ aws kms put-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --policy file://snapshotKey.json
```

Etapa 3: criar política de eventos de cópia entre contas (conta de destino)

Na conta de destino, crie uma política de eventos de cópia entre contas que copiará automaticamente os snapshots compartilhados pelas contas de origem necessárias.

Essa política só é executada na conta de destino quando uma das contas de origem especificadas compartilha o snapshot com a conta.

Use um dos seguintes métodos para criar a política de eventos de cópia entre contas.

Console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Na tela Select policy type (Selecionar tipo de política), escolha Cross-account copy event policy (Cópia de política de eventos entre contas) e depois Next (Próximo).
4. Em Policy description (Descrição da política), insira uma breve descrição da política.
5. Em Policy tags (Etiquetas de políticas), adicione as etiquetas a serem aplicadas na política de ciclo de vida. É possível usar essas etiquetas para identificar e categorizar suas políticas.
6. Na seção Event settings (Configurações de evento), defina o evento de compartilhamento de snapshots que fará com que a política seja executada. Faça o seguinte:

    a. Em Contas de compartilhamento, especifique as AWS contas de origem das quais você deseja copiar os instantâneos compartilhados. Escolha Adicionar conta, insira o ID da AWS conta de 12 dígitos e escolha Adicionar.

b. Em Filter by description (Filtrar por descrição), insira a descrição necessária do snapshot usando uma expressão regular. Somente os snapshots que são compartilhados pelas contas de origem especificadas e que tenham descrições que correspondam ao filtro especificado são copiados pela política. Para obter mais informações, consulte Especificar filtros de descrição de snapshot.

7. Para a IAM role (função do IAM), escolha a função do IAM que tem permissões para executar ações de cópia de snapshots. Para usar a função padrão fornecida pelo Amazon Data Lifecycle Manager, escolha Default role (Função padrão). Se preferir, para usar uma função do IAM personalizada criada anteriormente, selecione Choose another role (Escolher outra função) e selecione a função a ser usada.

   Se você estiver copiando snapshots criptografados, conceda as permissões de função do IAM selecionadas para usar a Chave do KMS de criptografia usada para criptografar o volume de origem. Da mesma forma, se você estiver criptografando o snapshot na região de destino usando uma Chave do KMS diferente, deverá conceder a permissão de função do IAM para usar a Chave do KMS de destino. Para obter mais informações, consulte Etapa 4: permitir que a função do IAM use as Chaves do KMS necessárias (conta de destino).

8. Na seção Copy action (Copiar ação), defina as ações de cópia de snapshots que a política deve executar quando for ativada. A política pode copiar snapshots para até três regiões. Especifique uma regra de cópia separada para cada região de destino. Para cada regra que você adicionar, faça o seguinte:

   a. Para Name (Nome), insira um nome descritivo para a ação de cópia.

   b. Em Target Region (Região de destino), selecione a região para a qual deseja copiar os snapshots.

   c. Em Expire, especifique por quanto tempo manter as cópias de snapshot na região de destino após a criação.

   d. Para criptografar a cópia do snapshot, Em Encryption (Criptografia), selecione Enable encryption (Habilitar criptografia). Se o snapshot de origem estiver criptografado ou se a criptografia por padrão estiver habilitada para a sua conta, a cópia do snapshot será sempre criptografada, mesmo que você não habilite a criptografia aqui. Se o snapshot de origem não estiver criptografado e a criptografia por padrão não estiver habilitada para sua conta, será possível optar por ativar ou desativar a criptografia. Se você habilitar a criptografia, mas não especificar uma Chave do KMS, os snapshots serão criptografados usando a Chave do KMS de criptografia padrão em cada região de

destino. Se você especificar uma Chave do KMS para a região de destino, deverá ter acesso à Chave do KMS.

9. Para adicionar outras ações de cópia de snapshot, escolha Add New Regions (Adicionar novas regiões).
10. Em Policy status after creation (Status da política após a criação), selecione Enable policy (Habilitar política) para iniciar as execuções da política no próximo horário agendado ou Disable policy (Desabilitar política) para impedir que a política seja executada. Se você não habilitar a política agora, ela não começará a copiar snapshots até que você a ative manualmente após a criação.
11. Escolha Create policy (Criar política).

Command line

Use o comando create-lifecycle-policy para criar uma política de ciclo de vida. Para criar uma política de eventos de cópia entre contas, para `PolicyType`, especifique `EVENT_BASED_POLICY`.

Por exemplo, o comando a seguir cria uma política de eventos de cópia entre contas na conta de destino `222222222222`. A política copia snapshots que são compartilhados pela conta de origem `111111111111`. A política copia snapshots para `sa-east-1` e `eu-west-2`. Os snapshots copiados para `sa-east-1` são criptografados e retidos por 3 dias. Os snapshots copiados para `eu-west-2` são criptografados usando a Chave do KMS `8af79514-350d-4c52-bac8-8985e84171c7` e são retidos por 1 mês. A política usa a função padrão do IAM.

```
$ aws dlm create-lifecycle-policy \
    --description "Copy policy" \
    --state ENABLED \
    --execution-role-arn arn:aws:iam::222222222222:role/service-role/
AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

O exemplo a seguir mostra o conteúdo do arquivo `policyDetails.json`.

```
{
    "PolicyType" : "EVENT_BASED_POLICY",
    "EventSource" : {
        "Type" : "MANAGED_CWE",
        "Parameters": {
            "EventType" : "shareSnapshot",
```

```
            "SnapshotOwner": ["111111111111"]
        }
    },
    "Actions" : [{
        "Name" :"Copy Snapshot to Sao Paulo and London",
        "CrossRegionCopy" : [{
            "Target" : "sa-east-1",
             "EncryptionConfiguration" : {
                 "Encrypted" : false
             },
             "RetainRule" : {
             "Interval" : 3,
            "IntervalUnit" : "DAYS"
            }
        },
        {
            "Target" : "eu-west-2",
            "EncryptionConfiguration" : {
                 "Encrypted" : true,
                 "CmkArn" : "arn:aws:kms:eu-
west-2:222222222222:key/8af79514-350d-4c52-bac8-8985e84171c7"
            },
            "RetainRule" : {
                "Interval" : 1,
                "IntervalUnit" : "MONTHS"
            }
        }]
    }]
}
```

Se a solicitação for bem-sucedida, o comando retornará o ID da política recém-criada. O seguinte é um exemplo de saída.

```
{
    "PolicyId": "policy-9876543210abcdef0"
}
```

Etapa 4: permitir que a função do IAM use as Chaves do KMS necessárias (conta de destino)

Se você estiver copiando snapshots criptografados, deverá conceder à função do IAM (que você selecionou na etapa anterior) permissões para usar a chave gerenciada pelo cliente que foi usada para criptografar o volume de origem.

> **Note**
> Execute esta etapa somente se você estiver copiando snapshots criptografados. Se você estiver copiando snapshots não criptografados, ignore esta etapa.

Use um dos métodos a seguir para adicionar as políticas necessárias à função do IAM.

Console

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Settings (Configurações). Pesquise e selecione a função do IAM selecionada ao criar a política de eventos de cópia entre contas na etapa anterior. Se você optar por usar a função padrão, a função será nomeada AWSDataLifecycleManagerDefaultRole.
3. Escolha Add inline policy (Adicionar política em linha) e, em seguida, a guia JSON.
4. Substitua a política existente pela a seguir, e especifique o ARN da chave de KMS que foi usada para criptografar os volumes de origem e que foi compartilhado com você pela conta de origem na Etapa 2.

   > **Note**
   > Se você estiver copiando de várias contas de origem, deverá especificar o ARN da chave de KMS correspondente a partir de cada conta de origem.

   No exemplo a seguir, a política concede a permissão de função do IAM para usar a Chave do KMS`1234abcd-12ab-34cd-56ef-1234567890ab`, que foi compartilhada pela conta de origem `111111111111` e Chave do KMS`4567dcba-23ab-34cd-56ef-0987654321yz` que existem na conta de destino `222222222222`.

   > **Tip**
   > Para seguir o princípio de menor privilégio, não permita acesso total a `kms:CreateGrant`. Em vez disso, use a chave de `kms:GrantIsForAWSResource` condição para permitir que o usuário crie

concessões na chave KMS somente quando a concessão for criada em nome do usuário por um AWS serviço, conforme mostrado no exemplo a seguir.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "kms:RevokeGrant",
               "kms:CreateGrant",
               "kms:ListGrants"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
               "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
           ],
           "Condition": {
               "Bool": {
                   "kms:GrantIsForAWSResource": "true"
               }
           }
       },
       {
           "Effect": "Allow",
           "Action": [
               "kms:Encrypt",
               "kms:Decrypt",
               "kms:ReEncrypt*",
               "kms:GenerateDataKey*",
               "kms:DescribeKey"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
               "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
           ]
       }
```

```
    ]
}
```

5. Escolha Review policy (Revisar política)
6. Para Name (Nome), insira um nome descritivo para a política e escolha Create policy (Criar política).

Command line

Usando seu editor de texto preferido, crie um novo arquivo JSON chamado `policyDetails.json`. Adicione a política a seguir e especifique o ARN da chave de KMS que foi usada para criptografar os volumes de origem e que foi compartilhada com você pela conta de origem na Etapa 2.

> **Note**
>
> Se você estiver copiando de várias contas de origem, deverá especificar o ARN da chave de KMS correspondente a partir de cada conta de origem.

No exemplo a seguir, a política concede a permissão de função do IAM para usar a Chave do KMS`1234abcd-12ab-34cd-56ef-1234567890ab`, que foi compartilhada pela conta de origem `111111111111` e Chave do KMS`4567dcba-23ab-34cd-56ef-0987654321yz` que existem na conta de destino `222222222222`.

> **Tip**
>
> Para seguir o princípio de menor privilégio, não permita acesso total a `kms:CreateGrant`. Em vez disso, use a chave de `kms:GrantIsForAWSResource` condição para permitir que o usuário crie concessões na chave KMS somente quando a concessão for criada em nome do usuário por um AWS serviço, conforme mostrado no exemplo a seguir.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
```

```
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

Salve e feche o arquivo. Em seguida, use o comando put-role-policy para adicionar a política à função do IAM.

Por exemplo

```
$ aws iam put-role-policy \
    --role-name AWSDataLifecycleManagerDefaultRole \
```

```
    --policy-name CopyPolicy \
    --policy-document file://AdminPolicy.json
```

Especificar filtros de descrição de snapshot

Quando você cria a política de cópia de snapshot na conta de destino, especifique um filtro de descrição de snapshot. O filtro de descrição do snapshot permite especificar um nível adicional de filtragem que permite controlar quais snapshots são copiados pela política. Isso significa que um snapshot só será copiado pela política se for compartilhado por uma das contas de origem especificadas e tiver uma descrição de snapshot que corresponda ao filtro especificado. Em outras palavras, se um snapshot for compartilhado por uma das contas de curso especificadas, mas não tiver uma descrição que corresponda ao filtro especificado, ele não será copiado pela política.

A descrição do filtro de snapshot deve ser especificada usando uma expressão regular. É um campo obrigatório ao criar políticas de eventos de cópia entre contas usando o console e a linha de comando. A seguir estão exemplos de expressões regulares que podem ser usadas:

- `.*`—Esse filtro corresponde a todas as descrições de snapshot. Se você usar essa expressão, a política copiará todos os snapshots compartilhados por uma das contas de origem especificadas.
- `Created for policy: policy-0123456789abcdef0.*`—Este filtro corresponde apenas aos snapshots criados por uma política com um ID de `policy-0123456789abcdef0`. Se você usar uma expressão como esta, apenas snapshots que são compartilhados com sua conta por uma das contas de origem especificadas e que foram criados por uma política com o ID especificado serão copiados pela política.
- `.*production.*`—Esse filtro corresponde a qualquer snapshot que tenha a palavra `production` em qualquer lugar em sua descrição. Se você usar essa expressão, a política copiará todos os snapshots compartilhados por uma das contas de origem especificadas e que tenham o texto especificado em sua descrição.

Considerações sobre políticas de cópia de snapshot entre contas

As seguintes considerações se aplicam às políticas de eventos de cópia entre contas:

- Você só pode copiar snapshots não criptografados ou criptografados usando uma chave gerenciada pelo cliente.
- É possível criar uma política de eventos de cópia entre contas para copiar snapshots compartilhados fora do Amazon Data Lifecycle Manager.

- Se você quiser criptografar snapshots na conta de destino, a função do IAM selecionada para a política de eventos de cópia entre contas deve ter permissão para usar a Chave do KMS necessária.

Recursos adicionais do

Para obter mais informações, consulte o blog Automatizando a cópia de snapshots criptografados do Amazon EBS entre AWS contas. AWS

Exibir, modificar e excluir políticas de ciclo de vida

Use os procedimentos a seguir para visualizar, modificar e excluir políticas de ciclo de vida existentes.

Tópicos

Visualizar políticas de ciclo de vida

Use um dos procedimentos a seguir para visualizar uma política de ciclo de vida.

Console

Como visualizar uma política de ciclo de vida

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic Block Store e, depois, Lifecycle Manager (Gerenciador de ciclo de vida).
3. Selecione o ID de uma política de ciclo de vida na lista.

Command line

Para obter informações resumidas sobre as políticas de ciclo de vida

Use o comando get-lifecycle-policies.

```
aws dlm get-lifecycle-policies
```

Para exibir informações sobre uma política de ciclo de vida específica

Use o comando get-lifecycle-policy. Em `--policy-id`, especifique o ID da política a ser exibida.

```
aws dlm get-lifecycle-policy --policy-id policy-0123456789abcdef0
```

Modificar políticas de ciclo de vida

Considerações sobre a modificação de políticas

- Se você modificar uma política de AMI ou snapshot removendo suas tags de destino, os volumes ou instâncias que possuam essas tags não serão mais gerenciados pela política.
- Se você alterar o nome da programação, os snapshots ou as AMIs criadas sob o antigo nome da programação não serão mais gerenciados pela política.
- Se você modificar uma programação de retenção baseada na idade para usar um novo intervalo de tempo, o novo intervalo será usado somente para novos snapshots ou AMIs criados após a alteração. A nova programação não afeta a programação de retenção de snapshots ou AMIs criados antes da alteração.
- Não é possível alterar a programação de retenção de uma política de baseada em contagem para baseada no tempo após a criação. Para fazer essa alteração, crie uma nova política.
- Se você desabilitar uma política com uma programação de retenção baseada em idade, os snapshots ou AMIs definidos para expirar enquanto a política estiver desativada serão mantidos indefinidamente. Exclua os snapshots ou cancelar o registro das AMIs manualmente. Quando você habilita a política novamente, o Amazon Data Lifecycle Manager retoma a exclusão de snapshots à medida que seus períodos de retenção expiram.
- Se você desabilitar uma política com um agendamento de retenção baseado em contagem, ela deixará de criar e excluir snapshots ou AMIs. Ao reabilitar a política, o Amazon Data Lifecycle Manager retoma a criação de snapshots e AMIs e retoma a exclusão de snapshots ou AMIs, conforme o limite de retenção é atingido.
- Se você desabilitar uma política que tenha uma política habilitada para arquivamento de snapshots, os snapshots que estiverem no nível de arquivamento no momento da desabilitação da política não serão mais gerenciados pelo Amazon Data Lifecycle Manager. Você deve excluir manualmente os snapshots, caso eles não sejam mais necessários.

- Se você habilitar o arquivamento de snapshots segundo uma programação baseada em contagem, a regra de arquivamento se aplicará a todos os novos snapshots criados e arquivados segundo a programação e também aos snapshots existentes que foram criados e arquivados anteriormente segundo a programação.
- Se você habilitar o arquivamento de snapshots segundo uma programação baseada em idade, a regra de arquivamento só se aplicará aos novos snapshots criados após a habilitação do arquivamento de snapshots. Os snapshots existentes criados antes da habilitação do arquivamento de snapshots continuarão sendo excluídos dos respectivos níveis de armazenamento, de acordo com a programação definida quando esses snapshots foram originalmente criados e arquivados.
- Se você desabilitar o arquivamento de snapshots para uma programação baseada em contagem, a programação interromperá imediatamente o arquivamento de snapshots. Os snapshots que foram previamente arquivados de acordo com a programação permanecerão no nível de arquivamento e não serão excluídos pelo Amazon Data Lifecycle Manager.
- Se você desabilitar o arquivamento de snapshots segundo uma programação baseada em idade, os snapshots criados pela política e que estão programados para serem arquivados serão excluídos permanentemente na data e hora de arquivamento programadas, conforme indicado pela tag `aws:dlm:expirationTime` do sistema.
- Se você desabilitar o arquivamento de snapshots segundo uma programação, a programação interromperá imediatamente o arquivamento de snapshots. Os snapshots que foram previamente arquivados de acordo com a programação permanecerão no nível de arquivamento e não serão excluídos pelo Amazon Data Lifecycle Manager.
- Se você modificar a contagem de retenção de arquivamento para uma programação baseada em contagem, a nova contagem de retenção incluirá os snapshots existentes que foram previamente arquivados segundo a programação.
- Se você modificar o período de retenção no arquivamento para um uma programação baseada em idade, o novo período de retenção só se aplicará aos snapshots que forem arquivados após a modificação da regra de retenção.

Use um dos procedimentos a seguir para modificar uma política de ciclo de vida.

Console

Para modificar uma política de ciclo de vida

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, escolha Elastic Block Store e, depois, Lifecycle Manager (Gerenciador de ciclo de vida).
3. Selecione uma política de ciclo de vida na lista.
4. Escolha Ações, Modificar política de ciclo de vida.
5. Modifique as configurações da política, conforme necessário. Por exemplo, é possível modificar a programação, adicionar ou remover tags ou habilitar e desabilitar a política.
6. Escolha Modificar política.

Command line

Use o comando update-lifecycle-policy para modificar informações em uma política de ciclo de vida. Para simplificar a sintaxe, este exemplo faz referência ao arquivo JSON `policyDetailsUpdated.json` que inclui os detalhes da política.

```
aws dlm update-lifecycle-policy \
    --state DISABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole" \
    --policy-details file://policyDetailsUpdated.json
```

Este é um exemplo do arquivo `policyDetailsUpdated.json`.

```
{
   "ResourceTypes":[
      "VOLUME"
   ],
   "TargetTags":[
      {
         "Key": "costcenter",
         "Value": "120"
      }
   ],
   "Schedules":[
      {
         "Name": "DailySnapshots",
         "TagsToAdd": [
            {
               "Key": "type",
               "Value": "myDailySnapshot"
```

```
            }
         ],
         "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
               "15:00"
            ]
         },
         "RetainRule": {
            "Count" :5
         },
         "CopyTags": false
      }
   ]
}
```

Para visualizar a política atualizada, use o comando `get-lifecycle-policy`. É possível ver que o estado, o valor da tag, o intervalo de snapshots e o horário de início do snapshot foram alterados.

Excluir políticas de ciclo de vida

Considerações sobre a modificação de políticas

- Se você excluir uma política de ciclo de vida, os snapshots ou AMIs criados por essa política não serão excluídos automaticamente. Se não precisar mais dos snapshots ou AMIs, é necessário excluí-los manualmente.
- Se você excluir uma política que tenha uma política habilitada para arquivamento de snapshots, os snapshots que estiverem no nível de arquivamento no momento da exclusão da política não serão mais gerenciados pelo Amazon Data Lifecycle Manager. Você deve excluir manualmente os snapshots, caso eles não sejam mais necessários.
- Se você excluir uma política com uma programação baseada em idade e habilitada para arquivamento, os snapshots criados pela política e que estão programados para serem arquivados serão excluídos permanentemente na data e hora de arquivamento programadas, conforme indicado pela tag `aws:dlm:expirationtime`do sistema.

Use um dos procedimentos a seguir para excluir uma política de ciclo de vida.

Console

Para excluir uma política de ciclo de vida

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic Block Store e, depois, Lifecycle Manager (Gerenciador de ciclo de vida).
3. Selecione uma política de ciclo de vida na lista.
4. Escolha Ações, Excluir política de ciclo de vida.
5. Quando a confirmação for solicitada, escolha Excluir política.

Command line

Use o comando delete-lifecycle-policy para excluir uma política de ciclo de vida e liberar as tag de destino especificadas na política para reutilização.

> **Note**
> É possível excluir snapshots criados somente por Amazon Data Lifecycle Manager.

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

A Referência de API do Amazon Data Lifecycle Manager fornece as descrições e a sintaxe de cada uma das ações e dos tipos de dados para a API de consulta do Amazon Data Lifecycle Manager.

Como alternativa, você pode usar um dos AWS SDKs para acessar a API de uma forma adaptada à linguagem de programação ou plataforma que você está usando. Para obter mais informações, consulte AWS SDKs.

AWS Identity and Access Management

O acesso ao Amazon Data Lifecycle Manager exige credenciais. Essas credenciais devem ter permissões para acessar os recursos AWS , como instâncias, volumes, snapshots e AMIs. As seções a seguir fornecem detalhes sobre como você pode usar o AWS Identity and Access Management (IAM) e ajudam a proteger o acesso aos seus recursos.

Tópicos

AWS políticas gerenciadas

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns. AWS as políticas gerenciadas tornam mais eficiente a atribuição de permissões apropriadas a usuários, grupos e funções do que se você mesmo tivesse que escrever as políticas.

No entanto, você não pode alterar as permissões definidas nas políticas AWS gerenciadas. AWS ocasionalmente atualiza as permissões definidas em uma política AWS gerenciada. Quando isso ocorre, a atualização afetará todas as principais entidades (usuários, grupos e funções) às quais a política está anexada.

O Amazon Data Lifecycle Manager fornece políticas AWS gerenciadas para casos de uso comuns. Essas políticas tornam mais eficiente definir as permissões apropriadas e controlar o acesso aos seus recursos. As políticas AWS gerenciadas fornecidas pelo Amazon Data Lifecycle Manager foram projetadas para serem vinculadas às funções que você passa para o Amazon Data Lifecycle Manager.

Tópicos

AWSDataLifecycleManagerServiceRole

A AWSDataLifecycleManagerServiceRolepolítica fornece permissões apropriadas ao Amazon Data Lifecycle Manager para criar e gerenciar políticas de snapshot do Amazon EBS e políticas de eventos de cópia entre contas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
```

```
        }
    ]
}
```

AWSDataLifecycleManagerServiceRoleForAMIManagement

A AWSDataLifecycleManagerServiceRoleForAMIManagementpolítica fornece permissões apropriadas ao Amazon Data Lifecycle Manager para criar e gerenciar políticas de AMI baseadas no Amazon EBS-Backed.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
```

```
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

AWSDataLifecycleManagerSSMFullAccess

Fornece ao Amazon Data Lifecycle Manager permissão para realizar as ações do Systems Manager necessárias para executar scripts prévios e posteriores em todas as instâncias do Amazon EC2.

> **Important**
>
> A política gerenciada usa a chave de condição `aws:ResourceTag` para restringir o acesso a documentos do SSM específicos ao usar scripts prévios e posteriores. Para permitir que o Amazon Data Lifecycle Manager acesse os documentos do SSM, você deve garantir que eles estejam marcados com `DLMScriptsAccess:true`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSMReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "ssm:GetCommandInvocation",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "AllowTaggedSSMDocumentsOnly",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
        {
            "Sid": "AllowSpecificAWSOwnedSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
                "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA"
            ]
        },
        {
            "Sid": "AllowAllEC2Instances",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ]
        }
    ]
}
```

AWS atualizações de políticas gerenciadas

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços adicionam permissões adicionais a uma política AWS gerenciada para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e perfis) em que a política está anexada. É mais provável que os serviços atualizem uma política AWS gerenciada quando um novo recurso é lançado ou quando novas operações são disponibilizadas. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

A tabela a seguir fornece detalhes sobre as atualizações das políticas AWS gerenciadas do Amazon Data Lifecycle Manager desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS em Histórico de documentos do Guia do usuário do Amazon EBS.

Alteração	Descrição	Data
AWSDataLifecycleManagerSSMFullAccess—Atualizou as permissões da política.	Atualizada a política para garantir compatibilidade com snapshots consistentes com a aplicação para o SAP HANA usando o documento do SSM `AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA` .	17 de novembro de 2023
AWSDataLifecycleMa	O Amazon Data Lifecycle	7 de novembro de 2023

Alteração	Descrição	Data
nagerSSMFullAccess— Foi adicionada uma nova política AWS gerenciada.	Manager adicionou a política gerenciada. AWSDataLifecycleManagerSSMFullAccess AWS	
AWSDataLifecycleManagerServiceRole— Permissões adicionadas para oferecer suporte ao arquivamento de instantâneos.	O Amazon Data Lifecycle Manager adicionou as ações `ec2:ModifySnapshotTier` e `ec2:DescribeSnapshotTierStatus` para conceder permissão às políticas de snapshots para arquivar snapshots e verificar seu status de arquivamento.	30 de setembro de 2022

Alteração	Descrição	Data
AWSDataLifecycleManagerServiceRoleForAMIManagement—Permissões adicionadas para dar suporte à descontinuação da AMI.	O Amazon Data Lifecycle Manager adicionou as ações `ec2:EnableImageDeprecation` e `ec2:DisableImageDeprecation` para conceder permissão de políticas de AMI apoiadas pelo EBS para habilitar e desabilitar a defasagem da AMI.	23 de agosto de 2021
O Amazon Data Lifecycle Manager começou a monitorar alterações	O Amazon Data Lifecycle Manager começou a monitorar as alterações em suas políticas gerenciadas. AWS	23 de agosto de 2021

Funções de serviço da IAM

Uma função AWS Identity and Access Management (IAM) é semelhante à de um usuário, pois é uma AWS identidade com políticas de permissões que determinam o que a identidade pode ou não fazer AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, o propósito do perfil é ser assumido por qualquer pessoa que precisar dele. Uma função de serviço é uma função que um AWS serviço assume para realizar ações em seu nome. Como um serviço que executa as operações de backup para você, o Amazon Data Lifecycle Manager exige que você atribua uma função a ele ao executar operações de política para você. Para obter mais informações sobre funções do IAM, consulte Funções do IAM no Guia do usuário do IAM.

A função que você passa para o Amazon Data Lifecycle Manager deve ter uma política do IAM com as permissões que possibilitam que o Amazon Data Lifecycle Manager execute ações associadas a operações de política, como criar snapshots e AMIs, copiar snapshots e AMIs, excluir snapshots e cancelar o registro de AMIs. Diferentes permissões são necessárias para cada um dos tipos de política do Amazon Data Lifecycle Manager. A função também deve ter o Amazon Data Lifecycle Manager listado como uma entidade confiável, o que permite que o Amazon Data Lifecycle Manager assuma a função.

Tópicos

Funções de serviço padrão para o Amazon Data Lifecycle Manager

O Amazon Data Lifecycle Manager usa as seguintes funções de serviço padrão:

- AWSDataLifecycleManagerDefaultRole—função padrão para gerenciar instantâneos. Ele confia apenas no serviço `dlm.amazonaws.com` para assumir a função e permite que o Amazon Data Lifecycle Manager execute as ações exigidas pelas políticas de cópia de snapshot e de snapshot entre contas em seu nome. Essa função usa a política `AWSDataLifecycleManagerServiceRole` AWS gerenciada.

> **Note**
>
> O formato do ARN da função é diferente dependendo se ela foi criada usando o console ou a AWS CLI. Se a função foi criada usando o console, o formato do ARN é `arn:aws:iam::`*`account_id`*`:role/service-`

`role/AWSDataLifecycleManagerDefaultRole`. Se a função foi criada usando o AWS CLI, o formato ARN é. `arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole`

- AWSDataLifecycleManagerDefaultRoleForAMIManagement—função padrão para gerenciar AMIs. Ela confia apenas no serviço `dlm.amazonaws.com` para assumir a função e permite que o Amazon Data Lifecycle Manager execute as ações exigidas pelas políticas de AMI apoiadas pelo EBS para você. Essa função usa a política `AWSDataLifecycleManagerServiceRoleForAMIManagement` AWS gerenciada.

Se você estiver usando o console do Amazon Data Lifecycle Manager, o Amazon Data Lifecycle Manager AWSDataLifecycleManagerDefaultRolecria automaticamente a função de serviço na primeira vez que você cria uma política de cópia de snapshot ou de snapshot entre contas, e cria automaticamente a função de serviço na primeira vez que você AWSDataLifecycleManagerDefaultRoleForAMIManagementcria uma política de AMI apoiada pelo EBS.

Se não estiver usando o console, será possível criar as funções de serviço manualmente usando o comando create-default-role. Para`--resource-type`, especifique `snapshot` para criar AWSDataLifecycleManagerDefaultRole ou `image` criar AWSDataLifecycleManagerDefaultRoleForAMIManagement.

```
$ aws dlm create-default-role --resource-type snapshot|image
```

Se você excluir essa função de serviço padrão e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta.

Funções de serviço personalizadas para o Amazon Data Lifecycle Manager

Como alternativa ao uso das funções de serviço padrão, é possível criar funções do IAM personalizadas com as permissões necessárias e selecioná-las ao criar uma política de ciclo de vida.

Para criar uma função do IAM personalizada

1. Crie funções com as seguintes permissões.

   - Permissões necessárias para gerenciar políticas de ciclo de vida de snapshot

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-
cwe.*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetCommandInvocation",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
```

```
            "Condition": {
                "StringNotLike": {
                    "aws:ResourceTag/DLMScriptsAccess": "false"
                }
            }
        }
    ]
}
```

- Permissões necessárias para gerenciar políticas de ciclo de vida da AMI

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
```

```
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

Para obter mais informações, consulte Criar uma função no Guia do usuário do IAM.

2. Adicione uma relação de confiança às funções.

   a. No console do IAM, selecione Roles (Funções).

   b. Selecione a função que você criou e, em seguida, escolha Relações de confiança.

   c. Escolha Edit Trust Relationship (Editar relação de confiança), adicione a seguinte política e, em seguida, escolha Update Trust Policy (Atualizar política de confiança).

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Principal": {
   "Service": "dlm.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
 }]
}
```

Recomendamos o uso das chaves de condição `aws:SourceAccount` e `aws:SourceArn` para se proteger contra O problema do agente confuso. Por exemplo, é possívelria adicionar o bloco de condições a seguir na política de confiança anterior. A `aws:SourceAccount` é a proprietária da política de ciclo de vida e o `aws:SourceArn`

é o ARN da política de ciclo de vida. Se você não souber o ID da política de ciclo de vida, poderá substituir essa parte do ARN por um curinga (`*`) e atualizar a política após criar a política de ciclo de vida.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:partition:dlm:region:account_id:policy/policy_id"
    }
}
```

Permissões para usuário

Um usuário da IAM deve ter as seguintes permissões para usar o Amazon Data Lifecycle Manager.

> **Note**
>
> - As permissões `ec2:DescribeAvailabilityZones`, `ec2:DescribeRegions`, `kms:ListAliases` e `kms:DescribeKey` são necessárias somente para usuários do console. Se o acesso ao console não for necessário, será possível remover as permissões.
> - O formato ARN da AWSDataLifecycleManagerDefaultRolefunção difere dependendo se ela foi criada usando o console ou o. AWS CLI Se a função foi criada usando o console, o formato do ARN é `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`. Se a função foi criada usando o AWS CLI, o formato ARN é A política `arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole` a seguir pressupõe que a função foi criada usando o. AWS CLI

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "dlm:*",
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::accound_id:role/service-role/
AWSDataLifecycleManagerDefaultRole",
                "arn:aws:iam::accound_id:role/service-role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement"
                ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeRegions",
                "kms:ListAliases",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações, consulte Alteração de permissões para um usuário no Guia do usuário do IAM.

Permissões para criptografia

Considere o seguinte ao trabalhar com o Amazon Data Lifecycle Manager e recursos criptografados.

- Se o volume de origem estiver criptografado, certifique-se de que as funções padrão do Amazon Data Lifecycle Manager (AWSDataLifecycleManagerDefaultRolee AWSDataLifecycleManagerDefaultRoleForAMIManagement) tenham permissão para usar as chaves KMS usadas para criptografar o volume.
- Se você habilitar Cross Region copy (Cópia entre regiões) para snapshots não criptografados ou AMIs apoiadas por snapshots não criptografados e optar por ativar a criptografia na região de

destino, verifique se as funções padrão têm permissão para usar a Chave do KMS necessária para executar a criptografia na região de destino.

- Se você habilitar a Cross Region copy (Cópia entre regiões) para snapshots criptografados ou AMIs apoiadas por snapshots criptografados, verifique se as funções padrão têm permissão para usar as Chaves do KMS de origem e de destino.
- Se você habilitar o arquivamento de snapshots para snapshots criptografados, certifique-se de que a AWSDataLifecycleManagerDefaultRolefunção padrão do Amazon Data Lifecycle Manager () tenha permissão para usar a chave KMS usada para criptografar o snapshot.

Para obter mais informações, consulte Como permitir que usuários em outras contas usem uma chave do KMS no Guia do desenvolvedor do AWS Key Management Service .

Monitorar o ciclo de vida de snapshots e AMIs

É possível usar os seguintes recursos para monitorar o ciclo de vida de seus snapshots e AMIs.

Recursos

- Console e AWS CLI
- AWS CloudTrail
- Monitore suas políticas usando CloudWatch Eventos
- Monitore suas políticas usando a Amazon CloudWatch

Console e AWS CLI

É possível visualizar as políticas de ciclo de vida usando o console do Amazon EC2 ou a AWS CLI. Cada snapshot e AMI criada por uma política possui um timestamp e tags relacionadas à política. É possível filtrar snapshots e AMIs usando tags para verificar se seus backups estão sendo criados conforme o esperado. Para obter informações sobre a visualização de políticas de ciclo de vida usando o console, consulte Visualizar políticas de ciclo de vida.

AWS CloudTrail

Com AWS CloudTrail, você pode monitorar a atividade do usuário e o uso da API para demonstrar conformidade com políticas internas e padrões regulatórios. Para mais informações, consulte o Guia do usuário do AWS CloudTrail.

Monitore suas políticas usando CloudWatch Eventos

O Amazon EBS e o Amazon Data Lifecycle Manager geram eventos relacionados às ações das políticas de ciclo de vida. Você pode usar o AWS Lambda Amazon CloudWatch Events para gerenciar notificações de eventos de forma programática. Os eventos são emitidos com base no melhor esforço. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Events.

Os seguintes eventos estão disponíveis:

> **Note**
>
> Nenhum evento é emitido para ações de política de ciclo de vida da AMI.

- `createSnapshot`: um evento do Amazon EBS emitido quando uma ação `CreateSnapshot` é bem-sucedida ou falha. Para ter mais informações, consulte Amazon EventBridge para Amazon EBS.
- `DLM Policy State Change`: um evento do Amazon Data Lifecycle Manager emitido quando uma política de ciclo de vida entra em um estado de erro. O evento contém uma descrição do que causou o erro.

  O exemplo a seguir mostra um evento em que as permissões concedidas pela função do IAM não são suficientes.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail": {
        "state": "ERROR",
        "cause": "Role provided does not have sufficient permissions",
```

```
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
}
```

O exemplo a seguir mostra um evento em que um limite é excedido.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail":{
        "state": "ERROR",
        "cause": "Maximum allowed active snapshot limit exceeded",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
}
```

- `DLM Pre Post Script Notification`: um evento que é emitido quando um prévio ou posterior é iniciado, é bem-sucedido ou falha.

  Veja a seguir um exemplo de evento quando um backup do VSS é bem-sucedido.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "DLM Pre Post Script Notification",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2023-10-27T22:04:52Z",
    "region": "us-east-1",
    "resources": ["arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef"],
    "detail": {
        "script_stage": "",
```

```
        "result": "success",
        "cause": "",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef",
        "execution_handler": "AWS_VSS_BACKUP",
        "source": "arn:aws:ec2:us-east-1:123456789012:instance/i-01234567890abcdef",
        "resource_type": "EBS_SNAPSHOT",
        "resources": [{
            "status": "pending",
            "resource_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
            "source": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-01234567890abcdef"
        }],
        "request_id": "a1b2c3d4-a1b2-a1b2-a1b2-a1b2c3d4e5f6",
        "start_time": "2023-10-27T22:03:29.370Z",
        "end_time": "2023-10-27T22:04:51.370Z",
        "timeout_time": ""
    }
}
```

Monitore suas políticas usando a Amazon CloudWatch

Você pode monitorar suas políticas de ciclo de vida do Amazon Data Lifecycle Manager usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. É possível usar essas métricas para ver exatamente quantos snapshots do Amazon EBS e AMIs baseadas no EBS são criados, excluídos e copiados por suas políticas ao longo do tempo. Também é possível definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos.

As métricas ficam armazenadas por um período de 15 meses para que você possa acessar informações históricas e obter uma compreensão melhor sobre a performance de suas políticas de ciclo de vida em um período prolongado.

Para obter mais informações sobre a Amazon CloudWatch, consulte o Guia CloudWatch do usuário da Amazon.

Tópicos

- Métricas compatíveis
- Veja CloudWatch métricas para suas políticas
- Métricas de gráfico para suas políticas

- Criar um CloudWatch alarme para uma política
- Exemplo de casos de uso
- Gerenciamento de políticas que relatam ações com falha

Métricas compatíveis

O namespace do `Data Lifecycle Manager` inclui as seguintes métricas das políticas de ciclo de vida do Amazon Data Lifecycle Manager. As métricas compatíveis diferem de acordo com o tipo de política.

Todas as métricas podem ser medidas na dimensão do `DLMPolicyId`. As estatísticas mais úteis são `sum` e `average`, e a unidade de medida é `count`.

Escolha uma guia para visualizar as métricas compatíveis com esse tipo de política.

EBS snapshot policies

Métrica	Descrição
`Resources Targeted`	O número de recursos de destino das tags especificadas em um snapshot ou política de AMI baseada no EBS.
`Snapshots CreateStarted`	O número de ações de criação de snapshots iniciadas por uma política de snapshot. Toda ação é registrada apenas uma vez, mesmo que haja várias tentativas subsequentes. Se uma ação de criação de snapshots falhar, o Amazon Data Lifecycle Manager enviará uma métrica `SnapshotsCreateFailed` .
`Snapshots CreateCompleted`	O número snapshots criados por uma política de snapshot. Inclui novas tentativas bem-sucedidas em até 60 minutos do horário agendado.
`Snapshots CreateFailed`	O número snapshots que uma política de snapshot não conseguiu criar. Inclui novas tentativas malsucedidas em até 60 minutos do horário agendado.

Métrica	Descrição
`SnapshotsSharedCompleted`	O número de de snapshots compartilhados entre contas por uma política de snapshot.
`SnapshotsDeleteCompleted`	O número de snapshots excluídos por um snapshot ou por uma política de AMI baseada no EBS. Essa métrica se aplica apenas aos snapshots criados pela política. Não se aplica a cópias de snapshots entre regiões criadas pela política. Essa métrica inclui snapshots que são excluídos quando uma política de AMI baseada no EBS cancela o registro de AMIs.
`SnapshotsDeleteFailed`	O número de snapshots que o snapshot ou a política de AMI baseada no EBS não conseguiu excluir. Essa métrica se aplica apenas aos snapshots criados pela política. Não se aplica a cópias de snapshots entre regiões criadas pela política. Essa métrica inclui snapshots que são excluídos quando uma política de AMI baseada no EBS cancela o registro de AMIs.
`SnapshotsCopiedRegionStarted`	O número de ações de cópia de snapshots entre regiões iniciadas por uma política de snapshot.
`SnapshotsCopiedRegionCompleted`	O número de ações de cópias de snapshots entre regiões criadas por uma política de snapshot. Inclui novas tentativas bem-sucedidas em até 24 horas do horário agendado.
`SnapshotsCopiedRegionFailed`	O número de cópias de snapshots entre regiões que não foi possível criar por meio de uma política de snapshot. Inclui tentativas malsucedidas num prazo de 24 horas a partir do horário agendado.
`SnapshotsCopiedRegionDeleteCompleted`	O número de cópias de snapshots entre regiões excluídas, conforme designado pela regra de retenção, por uma política de snapshot.

Métrica	Descrição
`SnapshotsCopiedRegionDeleteFailed`	O número de cópias de snapshots entre regiões que não foi possível excluir, conforme designado pela regra de retenção, por meio de uma política de snapshot.
`snapshotsArchiveDeletionFailed`	O número de snapshots arquivados que o não puderam ser excluídos do nível de arquivamento por uma política de snapshot.
`snapshotsArchiveScheduled`	O número de snapshots que foram programados para serem arquivados por uma política de snapshot.
`snapshotsArchiveCompleted`	O número de snapshots que foram arquivados com sucesso por uma política de snapshot.
`snapshotsArchiveFailed`	O número snapshots que não puderam ser criados por uma política de snapshot.
`snapshotsArchiveDeletionCompleted`	O número de snapshots arquivados que foram excluídos com sucesso do nível de arquivamento por uma política de snapshot.
`PreScriptStarted`	O número de instâncias em que um script prévio foi iniciado com sucesso. Se novas tentativas de script estiverem habilitadas, essa métrica poderá ser emitida várias vezes por execução de política.
`PreScriptCompleted`	O número de instâncias em que um script prévio foi concluído com sucesso. A métrica é emitida mesmo que o script prévio seja concluído fora do período limite especificado. Se novas tentativas de script estiverem habilitadas, essa métrica poderá ser emitida várias vezes por execução de política.

Métrica	Descrição
`PreScript Failed`	O número de instâncias em que um script prévio não foi concluído com sucesso. A métrica é emitida mesmo que o script prévio seja concluído fora do período limite especificado. Se novas tentativas de script estiverem habilitadas, essa métrica poderá ser emitida várias vezes por execução de política.
`PostScrip tStarted`	O número de instâncias em que um script posterior foi iniciado com sucesso. Se novas tentativas de script estiverem habilitadas, essa métrica poderá ser emitida várias vezes por execução de política.
PostScriptConcluído	O número de instâncias em que um script posterior foi concluído com sucesso. A métrica é emitida mesmo que o script posterior seja concluído fora do período limite especificado. Se novas tentativas de script estiverem habilitadas, essa métrica poderá ser emitida várias vezes por execução de política.
PostScriptFalhou	O número de instâncias em que um script posterior não foi concluído com sucesso. A métrica é emitida mesmo que o script posterior seja concluído fora do período limite especificado. Se novas tentativas de script estiverem habilitadas, essa métrica poderá ser emitida várias vezes por execução de política.
`VSSBackup Started`	O número de instâncias em que um script do VSS foi iniciado com sucesso. Se novas tentativas de script estiverem habilitadas, essa métrica poderá ser emitida várias vezes por execução de política.

Métrica	Descrição
`VSSBackup Completed`	O número de instâncias em que um backup do VSS foi concluído com sucesso. A métrica é emitida mesmo que o backup do VSS seja concluído fora do período limite especificado. Se novas tentativas de script estiverem habilitadas, essa métrica poderá ser emitida várias vezes por execução de política.
`VSSBackup Failed`	O número de instâncias em que um backup do VSS não foi concluído com sucesso. A métrica é emitida mesmo que o backup do VSS seja concluído fora do período limite especificado. Se novas tentativas de script estiverem habilitadas, essa métrica poderá ser emitida várias vezes por execução de política.

EBS-backed AMI policies

As métricas a seguir podem ser usadas com políticas de AMI baseadas no EBS:

Métrica	Descrição
`Resources Targeted`	O número de recursos de destino das tags especificadas em um snapshot ou política de AMI baseada no EBS.
`Snapshots DeleteCompleted`	O número de snapshots excluídos por um snapshot ou por uma política de AMI baseada no EBS. Essa métrica se aplica apenas aos snapshots criados pela política. Não se aplica a cópias de snapshots entre regiões criadas pela política. Essa métrica inclui snapshots que são excluídos quando uma política de AMI baseada no EBS cancela o registro de AMIs.
`Snapshots DeleteFailed`	O número de snapshots que o snapshot ou a política de AMI baseada no EBS não conseguiu excluir. Essa métrica se aplica apenas aos

Métrica	Descrição
	snapshots criados pela política. Não se aplica a cópias de snapshots entre regiões criadas pela política. Essa métrica inclui snapshots que são excluídos quando uma política de AMI baseada no EBS cancela o registro de AMIs.
`SnapshotsCopiedRegionDeleteCompleted`	O número de cópias de snapshots entre regiões excluídas, conforme designado pela regra de retenção, por uma política de snapshot.
`SnapshotsCopiedRegionDeleteFailed`	O número de cópias de snapshots entre regiões que não foi possível excluir, conforme designado pela regra de retenção, por meio de uma política de snapshot.
`ImagesCreateStarted`	O número de CreateImageações iniciadas por uma política de AMI apoiada pelo EBS.
`ImagesCreateCompleted`	O número de AMIs criadas por uma política de AMI baseada no EBS.
`ImagesCreateFailed`	O número de AMIs que não foi possível criar por meio de uma política de AMI baseada pelo EBS.
`ImagesDeregisterCompleted`	O número de AMIs que tiveram o registro cancelado por uma política de AMI baseada no EBS.
`ImagesDeregisterFailed`	O número de AMIs cujo registro não foi possível cancelar por meio de uma política de AMI baseada no EBS.

Métrica	Descrição
`ImagesCopiedRegionStarted`	O número de ações de cópia entre regiões iniciadas por uma política de AMI baseada no EBS.
`ImagesCopiedRegionCompleted`	O número de cópias de AMIs entre regiões criadas por uma política de AMI baseada no EBS.
`ImagesCopiedRegionFailed`	O número de cópias de AMIs entre regiões que não foi possível criar por meio de uma política de AMI baseada no EBS.
`ImagesCopiedRegionDeregisterCompleted`	O número de cópias de AMIs entre regiões que tiveram o registro cancelado, conforme designado pela regra de retenção, por meio de uma política de AMI baseada no EBS.
`ImagesCopiedRegionDeregisteredFailed`	O número de cópias de AMIs entre regiões cujo registro não foi possível cancelar, conforme designado pela regra de retenção, por meio de uma política de AMI baseada no EBS.
`EnableImageDeprecationCompleted`	O número de AMIs que foram marcadas para defasagem por meio de uma política de AMI baseada no EBS.
`EnableImageDeprecationFailed`	O número de AMIs que não puderam ser marcadas para defasagem por meio de uma política de AMI baseada no EBS.

Métrica	Descrição
`EnableCopiedImageDeprecationCompleted`	O número de cópias AMI entre regiões que foram marcadas para defasagem por meio de uma política de AMI baseada no EBS.
`EnableCopiedImageDeprecationFailed`	O número de cópias AMI entre regiões que não puderam ser marcadas para defasagem por meio de uma política de AMI baseada no EBS.

Cross-account copy event policies

As seguintes métricas podem ser usadas com políticas de eventos de cópia entre contas:

Métrica	Descrição
`SnapshotsCopiedAccountStarted`	O número de ações de cópia de snapshots entre contas iniciadas por uma política de eventos de cópia entre contas.
`SnapshotsCopiedAccountCompleted`	O número de snapshots copiados de outra conta por uma política de eventos de cópia entre contas. Inclui novas tentativas bem-sucedidas em até 24 horas do horário agendado.
`SnapshotsCopiedAccountFailed`	O número de snapshots que não foi possível copiar de outra conta por meio de uma política de eventos de cópia entre contas. Inclui tentativas malsucedidas num prazo de 24 horas do horário agendado.
`SnapshotsCopiedAcc`	O número de cópias de snapshots entre regiões excluídas, conforme designado pela regra de retenção, por uma política de evento de cópia entre contas.

Métrica	Descrição
`ountDeleteCompleted`	
`SnapshotsCopiedAccountDeleteFailed`	O número de cópias de snapshots entre regiões que não foi possível excluir, conforme designado pela regra de retenção, por meio de uma política de evento de cópia entre contas.

Veja CloudWatch métricas para suas políticas

Você pode usar as ferramentas AWS Management Console ou a linha de comando para listar as métricas que o Amazon Data Lifecycle Manager envia para a Amazon. CloudWatch

Amazon EC2 console

Para visualizar as métricas usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Gerenciador de ciclo de vida.
3. Selecione uma política na grade e, em seguida, escolha a guia Monitoramento.

CloudWatch console

Para visualizar métricas usando o CloudWatch console da Amazon

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Selecione o namespace do EBS e selecione as métricas do Data Lifecycle Manager.

AWS CLI

Para listar todas as métricas disponíveis para o Amazon Data Lifecycle Manager

Use o comando list-metrics.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS
```

Para listar todas as métricas para uma política específica

Use o comando list-metrics e especifique a dimensão `DLMPolicyId`.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --dimensions Name=DLMPolicyId,Value=policy-abcdef01234567890
```

Para listar uma métrica única em todas as políticas

Use o comando list-metrics e especifique a opção `--metric-name`.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --metric-name SnapshotsCreateCompleted
```

Métricas de gráfico para suas políticas

Depois que criar uma política, é possível abrir o console do Amazon EC2 e ver os gráficos de monitoramento para a instância na guia Monitoramento. Cada gráfico se baseia em uma das métricas disponíveis do Amazon EC2.

As métricas de gráficos a seguir estão disponíveis:

- Recursos direcionados (com base em `ResourcesTargeted`)
- Criação de snapshots iniciada (com base em `SnapshotsCreateStarted`)
- Criação de snapshots concluída (com base em `SnapshotsCreateCompleted`)
- Falha na criação de snapshots (com base em `SnapshotsCreateFailed`)
- Compartilhamento de snapshots concluído (com base em `SnapshotsSharedCompleted`)
- Exclusão de snapshot concluída (com base em `SnapshotsDeleteCompleted`)
- Falha na exclusão de snapshots (com base em `SnapshotsDeleteFailed`)
- Cópia de snapshots entre regiões iniciada (com base em `SnapshotsCopiedRegionStarted`)
- Cópia de snapshots entre regiões concluída (com base em `SnapshotsCopiedRegionCompleted`)

- Falha na cópia de snapshots entre regiões (com base em `SnapshotsCopiedRegionFailed`)
- Exclusão da cópia de snapshots entre regiões concluída (com base em `SnapshotsCopiedRegionDeleteCompleted`)
- Falha na exclusão da cópia de snapshots entre regiões (com base em `SnapshotsCopiedRegionDeleteFailed`)
- Cópia de snapshots entre contas iniciada (com base em `SnapshotsCopiedAccountStarted`)
- Cópia de snapshots entre contas concluída (com base em `SnapshotsCopiedAccountCompleted`)
- Falha na cópia de snapshots entre contas (com base em `SnapshotsCopiedAccountFailed`)
- Exclusão de cópia de snapshots entre contas concluída (com base em `SnapshotsCopiedAccountDeleteCompleted`)
- Falha na exclusão de cópia de snapshots entre contas (com base em `SnapshotsCopiedAccountDeleteFailed`)
- Criação de AMI iniciada (com base em `ImagesCreateStarted`)
- Criação de AMI concluída (com base em `ImagesCreateCompleted`)
- Falha na criação de AMI (com base em `ImagesCreateFailed`)
- Cancelamento de registro de AMI concluído (com base em `ImagesDeregisterCompleted`)
- Falha no cancelamento do registro da AMI (com base em `ImagesDeregisterFailed`)
- Cópia de AMI entre regiões iniciada (com base em `ImagesCopiedRegionStarted`)
- Cópia de AMI entre regiões concluída (com base em `ImagesCopiedRegionCompleted`)
- Falha na cópia de AMI entre regiões (com base em `ImagesCopiedRegionFailed`)
- Cancelamento de registro de cópia de AMI entre regiões concluída (com base em `ImagesCopiedRegionDeregisterCompleted`)
- Falha no cancelamento de registro da cópia de AMI entre regiões (com base em `ImagesCopiedRegionDeregisteredFailed`)
- AMI para habilitar defasagem concluído (com base em `EnableImageDeprecationCompleted`)
- Falha na AMI para habilitar defasagem (com base em `EnableImageDeprecationFailed`)
- Cópia da AMI para habilitar defasagem entre regiões concluída (com base em `EnableCopiedImageDeprecationCompleted`)
- Falha na cópia da AMI para habilitar defasagem entre regiões (com base em `EnableCopiedImageDeprecationFailed`)

Criar um CloudWatch alarme para uma política

Você pode criar um CloudWatch alarme que monitore CloudWatch as métricas de suas políticas. CloudWatch enviará automaticamente uma notificação quando a métrica atingir um limite especificado por você. Você pode criar um CloudWatch alarme usando o CloudWatch console.

Para obter mais informações sobre a criação de alarmes usando o CloudWatch console, consulte o tópico a seguir no Guia do CloudWatch usuário da Amazon.

- Crie um CloudWatch alarme com base em um limite estático
- Crie um CloudWatch alarme com base na detecção de anomalias

Exemplo de casos de uso

Veja a seguir exemplos de casos de uso:

Tópicos

Exemplo 1: ResourcesTargeted métrica

É possível usar a métrica `ResourcesTargeted` para monitorar o número total de recursos de destino de uma política específica toda vez que ela é executada. Isso permite acionar um alarme quando o número de recursos de destino estiver abaixo ou acima do limite esperado.

Por exemplo, se você espera que sua política diária crie backups de não mais do que `50` volumes, é possível criar um alarme que envia uma notificação por e-mail quando a `sum` de `ResourcesTargeted` for maior que `50` pelo período de `1` hora. Dessa forma, é possível garantir que nenhum snapshot tenha sido criado inesperadamente de volumes que foram etiquetados de maneira incorreta.

É possível usar o seguinte comando para criar este alarme:

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name resource-targeted-monitor \
    --alarm-description "Alarm when policy targets more than 50 resources" \
    --metric-name ResourcesTargeted \
```

```
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 50 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Exemplo 2: SnapshotDeleteFailed métrica

É possível usar a métrica `SnapshotDeleteFailed` para monitorar falhas na exclusão de snapshots, conforme a regra de retenção de snapshots da política.

Por exemplo, se você tiver criado uma política que deve excluir snapshots automaticamente a cada 12 horas, será possível criar um alarme que notifique sua equipe de engenharia quando a `sum` de `SnapshotDeletionFailed` for maior que `0` pelo período de `1` hora. Isso pode ajudar a averiguar a retenção incorreta de snapshots e a garantir que os custos de armazenamento não aumentem por causa de snapshots desnecessários.

É possível usar o seguinte comando para criar este alarme:

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-deletion-failed-monitor \
    --alarm-description "Alarm when snapshot deletions fail" \
    --metric-name SnapshotsDeleteFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Exemplo 3: SnapshotsCopiedRegionFailed métrica

Use a métrica `SnapshotsCopiedRegionFailed` para identificar quando suas políticas apresentam falha ao copiar snapshots para outras regiões.

Por exemplo, se sua política copia snapshots entre regiões diariamente, é possível criar um alarme que envia um SMS para sua equipe de engenharia quando a `sum` de

`SnapshotCrossRegionCopyFailed` for maior que `0` pelo período de `1` hora. Isso pode ser útil para verificar se a política copiou corretamente os snapshots subsequentes na linhagem.

É possível usar o seguinte comando para criar este alarme:

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-copy-region-failed-monitor \
    --alarm-description "Alarm when snapshot copy fails" \
    --metric-name SnapshotsCopiedRegionFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Gerenciamento de políticas que relatam ações com falha

Para obter mais informações sobre o que fazer quando uma de suas políticas relata um valor inesperado diferente de zero para uma métrica de ação falhada, consulte o artigo O que devo fazer se o Amazon Data Lifecycle Manager reportar ações malsucedidas nas métricas? CloudWatch AWS Artigo do Knowledge Center.

Solução de problemas

A documentação a seguir pode ajudar a solucionar os problemas que você venha a encontrar.

Tópicos

- Erro: Role with name already exists

Erro: **`Role with name already exists`**

Descrição

Você recebe o erro `Role with name AWSDataLifecycleManagerDefaultRole already exists` ou `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` ao tentar criar uma política usando o console.

Causa

O formato do ARN do perfil padrão é diferente dependendo de ele ter sido criado usando o console ou a AWS CLI. Embora os ARNs sejam diferentes, os perfis usam o mesmo nome de perfil, o que resulta em um conflito de nomenclatura de perfil entre o console e a AWS CLI.

Solução

Para resolver esse problema, faça o seguinte:

1. (Para políticas de snapshot habilitadas somente para scripts anteriores e posteriores) Anexe manualmente a política AWSDataLifecycleManagerSSMFullAccess AWS gerenciada à função do AWSDataLifecycleManagerDefaultRoleIAM. Para obter mais informações, consulte Adicionar permissões de identidade do IAM.
2. Ao criar sua política do Amazon Data Lifecycle Manager, para a função do IAM, selecione Escolher outra função e, em seguida, selecione AWSDataLifecycleManagerDefaultRole(para uma política de snapshot) ou (para uma política de AWSDataLifecycleManagerDefaultRoleForAMIManagementAMI).
3. Continue criando a política normalmente.

Usar o APIs diretas do EBS para acessar o conteúdo de um snapshot do EBS

É possível usar as APIs diretas do Amazon Elastic Block Store (Amazon EBS) para criar snapshots do EBS, gravar dados diretamente nos snapshots, ler dados nos snapshots e identificar as diferenças ou alterações entre dois snapshots. Se você for um provedor independente de software (ISV) que oferece serviços de backup para o Amazon EBS, as APIs diretas do EBS tornarão mais eficiente e econômico rastrear alterações incrementais em seus volumes do EBS por meio de snapshots. Isso pode ser feito sem a necessidade de criar volumes de snapshots e, depois, usar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) para comparar as diferenças.

É possível criar snapshots incrementais diretamente de dados on-premises em volumes do EBS e na nuvem a ser usada para recuperação rápida de desastre. Com a capacidade de gravar e ler snapshots, é possível gravar seus dados on-premises em um snapshot do EBS durante um desastre. Depois da recuperação, você pode restaurá-lo novamente AWS ou localmente a partir do snapshot. Não é mais necessário criar e manter mecanismos complexos para copiar dados de e para o Amazon EBS.

Este guia do usuário fornece uma visão geral dos elementos que compõem as APIs diretas do EBS, e exemplos de como usá-los de maneira eficaz. Para obter mais informações sobre as ações, os tipos de dados, os parâmetros e os erros das APIs, consulte a referência de APIs diretas do EBS. Para obter mais informações sobre as AWS regiões, endpoints e cotas de serviço compatíveis com as APIs diretas do EBS, consulte endpoints e cotas do Amazon EBS no. Referência geral da AWS

Conteúdo

Como entender o APIs diretas do EBS

Veja a seguir os principais elementos que devem ser compreendidos antes de começar a usar as APIs diretas do EBS.

Snapshots

Os snapshots são o principal meio de fazer backup de dados de volumes do EBS. Com as APIs diretas do EBS, também é possível fazer backup de dados de seus discos on-premises para snapshots. Para economizar custos de armazenamento, os snapshots sucessivos são incrementais, contendo apenas os dados do volume que mudaram desde o snapshot anterior. Para ter mais informações, consulte Snapshots do Amazon EBS.

> **Note**
>
> As APIs diretas do EBS não oferecem suporte a snapshots públicos e a snapshots locais no Outposts.

Blocos

Um bloco é um fragmento de dados dentro de um snapshot. Cada snapshot pode conter milhares de blocos. Todos os blocos em um snapshot são de tamanho fixo.

Índices de bloco

Um índice de blocos é um índice lógico em unidades de 512 blocos KiB. Para identificar o índice de bloco, divida o deslocamento lógico dos dados no volume lógico pelo tamanho do bloco (deslocamento lógico de dados/524288). O deslocamento lógico dos dados deve ser 512 KiB alinhado.

Tokens de bloco

Um token de bloco é o hash de identificação de um bloco dentro de um snapshot e é usado para localizar os dados do bloco. Os tokens de bloco retornados pelas APIs diretas do EBS são temporários. Eles mudam no timestamp de expiração especificado para eles, ou se você executar outro ListSnapshotBlocks ou ListChangedBlocks solicitar o mesmo snapshot.

Soma de verificação

Uma soma de verificação é um dado de tamanho pequeno derivado de um bloco de dados com a finalidade de detectar erros apresentados durante sua transmissão ou armazenamento. As APIs diretas do EBS usam as somas de verificação para validar a integridade dos dados. Quando você lê dados de um snapshot do EBS, o serviço fornece somas de verificação SHA256 codificadas pelo Base64 para cada bloco de dados transmitidos, que é possível usar para validação. Ao gravar dados em um snapshot do EBS, forneça uma soma de verificação SHA256 codificada pelo Base64 para cada bloco de dados transmitidos. O serviço valida os dados recebidos usando a soma de verificação fornecida. Para obter mais informações, consulte Usar somas de verificação adiante neste guia.

Criptografia

A criptografia protege seus dados convertendo-os em código ilegível que só pode ser decifrado por pessoas que tiverem acesso à Chave do KMS usada para criptografá-los. É possível usar as APIs diretas do EBS para ler e gravar snapshots criptografados, mas há algumas limitações. Para obter mais informações, consulte Usar criptografia adiante neste guia.

Ações da API

As APIs diretas do EBS consistem em seis ações. Há três ações de leitura e três ações de gravação. As ações de leitura são:

- ListSnapshotBlocos — retorna os índices de blocos e os tokens de blocos no instantâneo especificado
- ListChangedBlocos — retorna os índices de blocos e os tokens de blocos que são diferentes entre dois instantâneos especificados do mesmo volume e linhagem de instantâneos.
- GetSnapshotBloco — retorna os dados em um bloco para o ID de snapshot, índice de bloco e token de bloco especificados.

As ações de gravação são:

- StartSnapshot— inicia um instantâneo, seja como um instantâneo incremental de um existente ou como um novo instantâneo. O instantâneo iniciado permanece em um estado pendente até ser concluído usando a CompleteSnapshot ação.
- PutSnapshotBloco — adiciona dados a um instantâneo iniciado na forma de blocos individuais. Especifique uma soma de verificação SHA256 codificada como Base64 para o bloco de dados

transmitido. O serviço valida a soma de verificação após a conclusão da transmissão. A solicitação falhará se a soma de verificação calculada pelo serviço não corresponder à que você especificou.

- CompleteSnapshot— conclui um snapshot iniciado que está em um estado pendente. Depois, os snapshots são alterados para um estado concluído.

Permissões do IAM para APIs diretas do EBS

Um usuário do precisa ter as políticas a seguir para usar as APIs diretas do EBS. Para obter mais informações, consulte Alterar permissões para um usuário.

Para mais informações sobre os recursos, ações e chaves contextuais de condição de APIs diretas do EBS para uso em políticas de permissão do IAM, consulte Ações, recursos e chaves de condição do Amazon Elastic Block Store na Referência de autorização do serviço.

> **Important**
>
> Tenha cuidado ao atribuir as seguintes políticas aos usuários do . Ao atribuir essas políticas, você pode conceder acesso a um usuário cujo acesso ao mesmo recurso é negado por meio das APIs do Amazon EC2, como as CopySnapshot ações ou. CreateVolume

Permissões para ler snapshots

A política a seguir permite que as APIs diretas do EBS de leitura sejam usadas em todos os snapshots em uma região específica. AWS Na política, substitua *<Region>* pela região do snapshot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
```

```
}
```

A política a seguir permite que a leitura das APIs diretas do EBS seja usada em snapshots com uma tag de chave/valor específica. Na política, substitua *<Key>* pelo valor de chave da tag e *<Value>* pelo valor da tag.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

A política a seguir permite que todas as APIs diretas do EBS de leitura sejam usadas em todos os snapshots da conta apenas dentro de um intervalo de tempo específico. Essa política autoriza o uso das APIs diretas do EBS baseadas na chave de condição global `aws:CurrentTime`. Na política, substitua o intervalo de data e hora mostrado pelo intervalo de data e hora da sua política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
```

```
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

Para obter mais informações, consulte Alteração de permissões para um usuário no Guia do usuário do IAM.

Permissões para gravar snapshots

A política a seguir permite que as APIs diretas de gravação do EBS sejam usadas em todos os snapshots em uma região específica. AWS Na política, substitua *<Region>* pela região do snapshot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
}
```

A política a seguir permite que a gravação das APIs diretas do EBS seja usada em snapshots com uma tag de chave/valor específica. Na política, substitua *<Key>* pelo valor de chave da tag e *<Value>* pelo valor da tag.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

A política a seguir permite que todas as APIs diretas do EBS sejam usadas. Ela também permite a ação `StartSnapshot` somente se um ID de snapshot pai for especificado. Portanto, essa política bloqueia a capacidade de iniciar novos snapshots sem o uso de um snapshot pai.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ebs:ParentSnapshot": "arn:aws:ec2:*::snapshot/*"
                }
            }
        }
    ]
}
```

A política a seguir permite que todas as APIs diretas do EBS sejam usadas. Ela também permite que apenas a chave de tag `user` seja criada para um novo snapshot. Essa política também garante que o usuário tenha acesso à criação de tags. A ação `StartSnapshot` é a única ação que pode especificar tags.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "user"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

A política a seguir permite que todas as APIs diretas do EBS de gravação sejam usadas em todos os snapshots da conta apenas dentro de um intervalo de tempo específico. Essa política autoriza o uso das APIs diretas do EBS baseadas na chave de condição global `aws:CurrentTime`. Na política, substitua o intervalo de data e hora mostrado pelo intervalo de data e hora da sua política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
```

```
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

Para obter mais informações, consulte Alteração de permissões para um usuário no Guia do usuário do IAM.

Permissões de uso AWS KMS keys

A política a seguir concede permissão para descriptografar um snapshot criptografado usando uma chave do KMS específica. Ela também concede permissão para criptografar novos snapshots usando a chave padrão do KMS para criptografia do EBS. Na política, <Region>substitua pela Região da chave KMS, `< AccountId >` pela ID da AWS conta da chave KMS e `< KeyId >` pela ID da chave KMS.

> **Note**
>
> Por padrão, todos os diretores da conta têm acesso à chave KMS AWS gerenciada padrão para a criptografia do Amazon EBS e podem usá-la para operações de criptografia e descriptografia do EBS. Se você estiver usando uma chave gerenciada pelo cliente, deverá criar uma nova política de chaves ou modificar a política de chaves existente para a chave gerenciada pelo cliente para conceder ao principal acesso à chave gerenciada pelo cliente. Para obter mais informações, consulte Políticas de chaves no AWS KMS no Guia do desenvolvedor do AWS Key Management Service .

> **Tip**
>
> Para seguir o princípio de menor privilégio, não permita acesso total a `kms:CreateGrant`. Em vez disso, use a chave de `kms:GrantIsForAWSResource` condição para permitir que o usuário crie concessões na chave KMS somente quando a concessão for criada em nome do usuário por um AWS serviço, conforme mostrado no exemplo a seguir.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncrypt*",
                "kms:CreateGrant",
                "ec2:CreateTags",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:<Region>:<AccountId>:key/<KeyId>",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

Para obter mais informações, consulte Alteração de permissões para um usuário no Guia do usuário do IAM.

Usar APIs diretas do EBS

Os tópicos a seguir mostram como ler e gravar snapshots usando as APIs diretas do EBS. Você pode ler e gravar instantâneos usando somente AWS APIs e AWS SDKs. AWS CLI Para obter mais informações, consulte:

- Instalando AWS CLI e configurando o AWS CLI
- Referência de APIs diretas do EBS
- AWS SDKs

> **Important**
>
> As APIs diretas do EBS exigem uma AWS assinatura Signature Version 4. Para ter mais informações, consulte Usar a assinatura do Signature versão 4..

Tópicos

Ler os snapshots com APIs diretas do EBS

As etapas a seguir descrevem como usar as APIs diretas do EBS para ler snapshots:

1. Use a ListSnapshotBlocks ação para visualizar todos os índices de blocos e tokens de blocos em um instantâneo. Ou use a ListChangedBlocks ação para visualizar somente os índices de blocos e os tokens de blocos que são diferentes entre dois instantâneos do mesmo volume e linhagem de instantâneos. Essas ações ajudam você a identificar os tokens e os índices de bloco dos blocos para os quais é possível querer obter dados.
2. Use a GetSnapshotBlock ação e especifique o índice do bloco e o token do bloco para o qual você deseja obter dados.

Os exemplos a seguir mostram como ler snapshots usando as APIs diretas do EBS.

Tópicos

- Obter dados de bloco de um snapshot

Listar blocos em um snapshot

AWS CLI

O comando de exemplo list-snapshot-blocks a seguir retorna os índices e os tokens de bloco dos blocos que estão no snapshot `snap-0987654321`. O parâmetro `--starting-block-index` limita os resultados para índices de bloco maiores que `1000`, e o parâmetro `--max-results` limita os resultados aos primeiros `100` blocos.

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-
index 1000 --max-results 100
```

A resposta de exemplo a seguir para o comando anterior lista os índices e os tokens de bloco no snapshot. Use o comando `get-snapshot-block` e especifique o índice e o token do bloco do qual você deseja obter dados. Os tokens de bloco são válidos até o tempo de expiração listado.

```
{
      "Blocks": [
          {
              "BlockIndex": 1001,
              "BlockToken": "AAABAV3/
PNhXOynVdMYHUpPsetaSvjLB1dtIGfbJv5OJ0sX855EzGTWos4a4"
          },
          {
              "BlockIndex": 1002,
              "BlockToken": "AAABATGQIgwr0WwIuqIMjCA/Sy7e/
YoQFZsHejzGNvjKauzNgzeI13YHBfQB"
          },
          {
              "BlockIndex": 1007,
              "BlockToken": "AAABAZ9CTuQtUvp/
dXqRWw4d07eOgTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"
          },
          {
              "BlockIndex": 1012,
              "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/
YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"
          },
          {
```

```
                "BlockIndex": 1030,
                "BlockToken": "AAABAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L
+CbXnvpkswA6iDID523d"
            },
            {
                "BlockIndex": 1031,
                "BlockToken": "AAABATgWZC0XcFwUKvTJbUXMiSPg59KVxJGL
+BWBClkw6spzCxJVqDVaTskJ"
            },
            ...
        ],
        "ExpiryTime": 1576287332.806,
        "VolumeSize": 32212254720,
        "BlockSize": 524288
    }
```

AWS API

O exemplo de solicitação de ListSnapshotblocos a seguir retorna os índices de blocos e os tokens de bloco dos blocos que estão no snapshot`snap-0acEXAMPLEcf41648`. O parâmetro `startingBlockIndex` limita os resultados para índices de bloco maiores que `1000`, e o parâmetro `maxResults` limita os resultados aos primeiros `100` blocos.

```
GET /snapshots/snap-0acEXAMPLEcf41648/blocks?maxResults=100&startingBlockIndex=1000
 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T231953Z
  Authorization: <Authentication parameter>
```

A resposta de exemplo a seguir para a solicitação anterior lista os índices e os tokens de bloco no snapshot. Use a GetSnapshotBlock ação e especifique o índice do bloco e o token do bloco para o qual você deseja obter dados. Os tokens de bloco são válidos até o tempo de expiração listado.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: d6e5017c-70a8-4539-8830-57f5557f3f27
  Content-Type: application/json
  Content-Length: 2472
  Date: Wed, 17 Jun 2020 23:19:56 GMT
  Connection: keep-alive
```

```
  {
      "BlockSize": 524288,
      "Blocks": [
          {
              "BlockIndex": 0,
              "BlockToken": "AAUBAcuWqOCnDNuKle11s7IIX6jp6FYcC/q8oT93913HhvLvA
+3JRrSybp/0"
          },
          {
              "BlockIndex": 1536,
              "BlockToken":
 "AAUBAWudwfmofcrQhGVlLwuRKm2b8ZXPiyrgoykTRC6IU1NbxKWDY1pPjvnV"
          },
          {
              "BlockIndex": 3072,
              "BlockToken":
 "AAUBAV7p6pC5fKAC7TokoNCtAnZhqq27u6YEXZ3MwRevBkDjmMx6iuA6tsBt"
          },
          {
              "BlockIndex": 3073,
              "BlockToken":
 "AAUBAbqt9zpqBUEvtO2HINAfFaWToOwlPjbIsQOlx6JUN/0+iMQl0NtNbnX4"
          },
          ...
      ],
      "ExpiryTime": 1.59298379649E9,
      "VolumeSize": 3
  }
```

Listar blocos diferentes entre dois snapshots

Lembre-se do seguinte ao fazer solicitações paginadas para listar os blocos alterados entre dois snapshots:

- A resposta pode incluir uma ou mais matrizes `ChangedBlocks` vazias. Por exemplo:
  - Snapshot 1: snapshot completo com 1000 blocos com índices de blocos `0` - 999.
  - Snapshot 2: snapshot incremental com apenas um bloco alterado com índice de bloco 999.

  Listar os blocos alterados para esses snapshot com `StartingBlockIndex = 0` e `MaxResults = 100` retorna uma matriz vazia de `ChangedBlocks`. É necessário solicitar os resultados

restantes usando `nextToken` até que o bloco alterado seja retornado no décimo conjunto de resultados, que inclui blocos com índices de blocos `900` - `999`.

- A resposta pode ignorar blocos não escritos nos snapshots. Por exemplo:
  - Snapshot 1: snapshot completo com 1000 blocos com índices de blocos `2000` - `2999`.
  - Snapshot 2: snapshot incremental com apenas um bloco alterado com índice de bloco `2000`.

  Listando os blocos alterados para esses snapshots com `StartingBlockIndex = 0` e`MaxResults = 100`, a resposta ignora os índices de blocos `0` - `1999` e inclui o índice de blocos`2000`. A resposta não incluirá matrizes `ChangedBlocks` vazias.

AWS CLI

O comando de exemplo list-changed-blocks a seguir retorna os índices e os tokens de bloco dos blocos que são diferentes entre os snapshots `snap-1234567890` e `snap-0987654321`. O parâmetro `--starting-block-index` limita os resultados para índices de bloco maiores que `0`, e o parâmetro `--max-results` limita os resultados aos primeiros `500` blocos.

```
aws ebs list-changed-blocks --first-snapshot-id snap-1234567890 --second-snapshot-
id snap-0987654321 --starting-block-index 0 --max-results 500
```

A resposta de exemplo a seguir para o comando anterior mostra que os índices de bloco 0, 6000, 6001, 6002 e 6003 são diferentes entre os dois snapshots. Além disso, os índices de bloco 6001, 6002 e 6003 existem somente no primeiro ID de snapshot especificado, e não no segundo ID de snapshot, porque não há um segundo token de bloco listado na resposta.

Use o comando `get-snapshot-block` e especifique o índice e o token do bloco do qual você deseja obter dados. Os tokens de bloco são válidos até o tempo de expiração listado.

```
{
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAABAVahm9SO60Dyi0ORySzn2ZjGjW/
KN3uygGlS0QOYWesbzBbDnX2dGpmC",
              "SecondBlockToken":
 "AAABAf8o0o6UFi1rDbSZGIRaCEdDyBu9TlvtCQxxoKV8qrUPQP7vcM6iWGSr"
          },
          {
              "BlockIndex": 6000,
```

```
              "FirstBlockToken": "AAABAbYSiZvJ0/
R9tz8suI8dSzecLjN4kkazK8inFXVintPkdaVFLfCMQsKe",
              "SecondBlockToken":
 "AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777elD9oVR"
          },
          {
              "BlockIndex": 6001,
              "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/
T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR"
          },
          {
              "BlockIndex": 6002,
              "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
          },
          {
              "BlockIndex": 6003,
              "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
          },
          ...
      ],
      "ExpiryTime": 1576308931.973,
      "VolumeSize": 32212254720,
      "BlockSize": 524288,
      "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVaO0zsPH/QM3Bi3zF//
O6Mdi/BbJarBnp8h"
  }
```

AWS API

O exemplo de solicitação de ListChangedblocos a seguir retorna os índices de blocos e os tokens de blocos que são diferentes entre instantâneos e. `snap-0acEXAMPLEcf41648` `snap-0c9EXAMPLE1b30e2f` O parâmetro `startingBlockIndex` limita os resultados para índices de bloco maiores que `0`, e o parâmetro `maxResults` limita os resultados aos primeiros `500` blocos.

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/changedblocks?
firstSnapshotId=snap-0acEXAMPLEcf41648&maxResults=500&startingBlockIndex=0 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232546Z
```

```
  Authorization: <Authentication parameter>
```

A resposta de exemplo a seguir para a solicitação anterior mostra que os índices de bloco `0`, `3072`, `6002` e `6003` são diferentes entre os dois snapshots. Além disso, os índices de bloco `6002` e `6003` existem somente no primeiro ID de snapshot especificado, e não no segundo ID de snapshot, porque não há um segundo token de bloco listado na resposta.

Use a ação `GetSnapshotBlock` e especifique o índice e o token do bloco do qual você deseja obter dados. Os tokens de bloco são válidos até o tempo de expiração listado.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: fb0f6743-6d81-4be8-afbe-db11a5bb8a1f
  Content-Type: application/json
  Content-Length: 1456
  Date: Wed, 17 Jun 2020 23:25:47 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAUBAVaWqOCnDNuKle11s7IIX6jp6FYcC/
tJuVT1GgP23AuLntwiMdJ+OJkL",
              "SecondBlockToken": "AAUBASxzy0Y0b33JVRLoYm3NOresCxn5RO+HVFzXW3Y/
RwfFaPX2Edx8QHCh"
          },
          {
              "BlockIndex": 3072,
              "FirstBlockToken":
 "AAUBAcHp6pC5fKAC7TokoNCtAnZhqq27u6fxRfZOLEmeXLmHBf2R/Yb24MaS",
              "SecondBlockToken":
 "AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid"
          },
          {
              "BlockIndex": 6002,
              "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
          },
          {
              "BlockIndex": 6003,
              "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
```

```
            },
            ...
        ],
        "ExpiryTime": 1.592976647009E9,
        "VolumeSize": 3
    }
```

Obter dados de bloco de um snapshot

AWS CLI

O comando de exemplo get-snapshot-block a seguir retorna os dados no índice de bloco `6001` com o token de bloco `AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR`, no snapshot `snap-1234567890`. Os dados binários serão enviados para o arquivo `data` no diretório `C:\Temp` em um computador Windows. Se você executar o comando em um computador Linux ou Unix, substitua o caminho de saída por `/tmp/data` para enviar os dados ao arquivo `data` no diretório `/tmp`.

```
aws ebs get-snapshot-block --snapshot-id snap-1234567890 --block-index 6001 --block-token AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR C:/Temp/data
```

A resposta de exemplo a seguir para o comando anterior mostra o tamanho dos dados retornados, a soma de verificação para validar os dados e o algoritmo da soma de verificação. Os dados binários são salvos automaticamente no diretório e no arquivo especificados no comando da solicitação.

```
{
        "DataLength": "524288",
        "Checksum": "cf0Y6/Fn0oFa4VyjQPOa/iD0zhTflPTKzxGv2OKowXc=",
        "ChecksumAlgorithm": "SHA256"
    }
```

AWS API

O exemplo de solicitação de GetSnapshotbloco a seguir retorna os dados no índice do bloco `3072` com o token do blocoAAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid, em um instantâneosnap-0c9EXAMPLE1b30e2f.

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/blocks/3072?
blockToken=AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232838Z
  Authorization: <Authentication parameter>
```

A resposta de exemplo a seguir para a solicitação anterior mostra o tamanho dos dados retornados, a soma de verificação para validar os dados e o algoritmo usado para gerar a soma de verificação. Os dados binários são transmitidos no corpo da resposta e são representados como `BlockData`no exemplo a seguir.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: 2d0db2fb-bd88-474d-a137-81c4e57d7b9f
  x-amz-Data-Length: 524288
  x-amz-Checksum: Vc0yY2j3qg8bUL9I6GQuI2orTudrQRBDMIhcy7bdEsw=
  x-amz-Checksum-Algorithm: SHA256
  Content-Type: application/octet-stream
  Content-Length: 524288
  Date: Wed, 17 Jun 2020 23:28:38 GMT
  Connection: keep-alive

  BlockData
```

Gravar os snapshots com APIs diretas do EBS

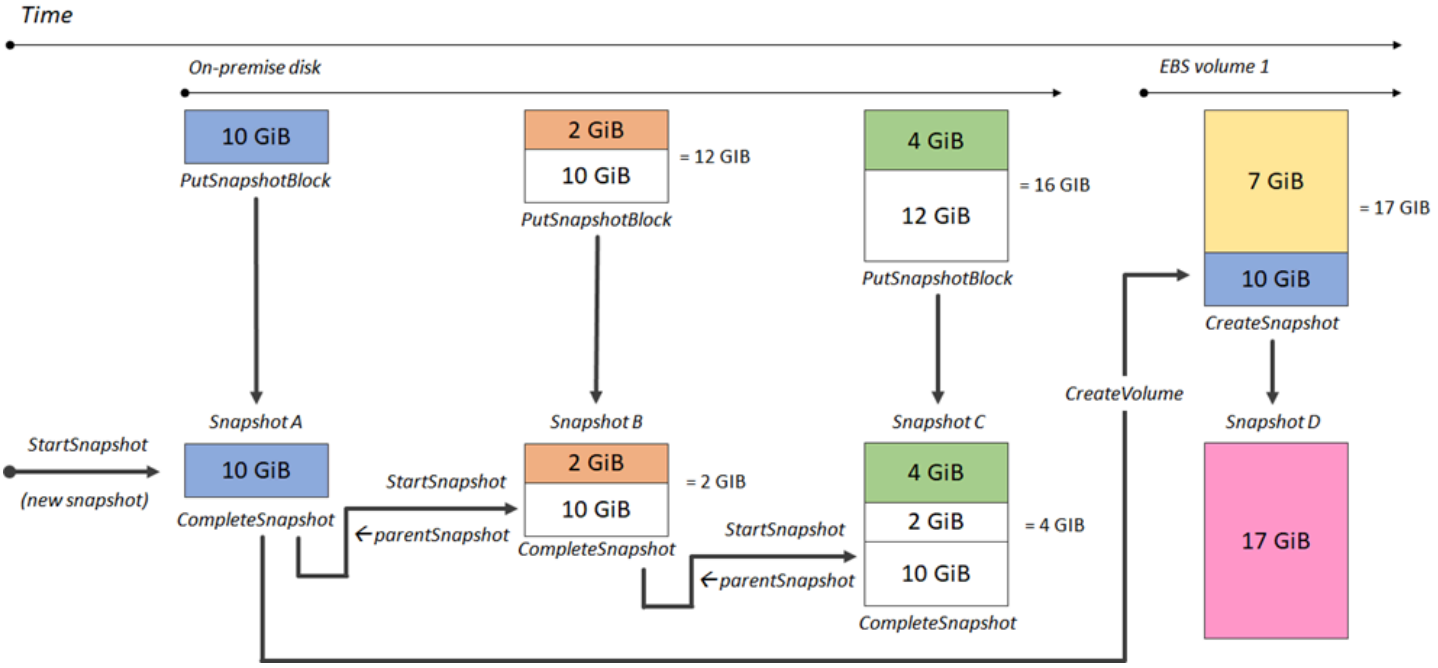
As etapas a seguir descrevem como usar as APIs diretas do EBS para gravar snapshots incrementais:

1. Use a StartSnapshot ação e especifique uma ID de instantâneo principal para iniciar um instantâneo como um instantâneo incremental de um existente ou omita a ID de instantâneo pai para iniciar um novo instantâneo. Essa ação retorna o novo ID de snapshot que está em estado pendente.
2. Use a PutSnapshotBlock ação e especifique a ID do instantâneo pendente para adicionar dados a ele na forma de blocos individuais. Especifique uma soma de verificação SHA256 codificada como Base64 para o bloco de dados transmitido. O serviço calcula a soma de verificação dos dados recebidos e os valida com relação à soma de verificação especificada. A ação falhará se as somas de verificação não corresponderem.

3. Quando terminar de adicionar dados ao instantâneo pendente, use a CompleteSnapshot ação para iniciar um fluxo de trabalho assíncrono que sela o instantâneo e o move para um estado concluído.

Repita essas etapas para criar um novo snapshot incremental usando o snapshot criado anteriormente como pai.

Por exemplo, no diagrama a seguir, o snapshot A é o primeiro novo snapshot iniciado. O snapshot A é usado como snapshot pai para iniciar o snapshot B. O snapshot B é usado como snapshot pai para iniciar e criar o snapshot C. Os snapshots A, B e C são snapshots incrementais. O snapshot A é usado para criar o volume 1 do EBS. O snapshot D é criado a partir do volume 1 do EBS. O snapshot D é um snapshot incremental de A; ele não é um snapshot incremental de B nem C.



Os exemplos a seguir mostram como gravar snapshots usando as APIs diretas do EBS.

Tópicos

- Iniciar um snapshot
- Inserir dados em um snapshot
- Concluir um snapshot

Iniciar um snapshot

AWS CLI

O comando de exemplo start-snapshot a seguir inicia um snapshot 8 GiB usando o snapshot `snap-123EXAMPLE1234567` como snapshot pai. O novo snapshot será um snapshot incremental do snapshot pai. O snapshot será movido para um estado de erro se não houver solicitações put ou complete feitas para o snapshot dentro do período limite especificado de `60` minutos. O token `550e8400-e29b-41d4-a716-446655440000` do cliente garante idempotência para a solicitação. Se o token do cliente for omitido, o AWS SDK gerará automaticamente um para você. Para obter mais informações sobre idempotência, consulte Idempotência para API StartSnapshot .

```
aws ebs start-snapshot --volume-size 8 --parent-snapshot snap-123EXAMPLE1234567 --
timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

O exemplo de resposta a seguir para o comando anterior mostra o ID do snapshot, o ID da conta da AWS , o status, o tamanho do volume em GiB e o tamanho dos blocos no snapshot. O snapshot é iniciado em estado `pending`. Especifique o ID do snapshot nos comandos `put-snapshot-block` subsequentes para gravar dados no snapshot, depois, use o comando `complete-snapshot` para concluir o snapshot e alterar seu status para `completed`.

```
{
    "SnapshotId": "snap-0aaEXAMPLEe306d62",
    "OwnerId": "111122223333",
    "Status": "pending",
    "VolumeSize": 8,
    "BlockSize": 524288
}
```

AWS API

O StartSnapshotexemplo de solicitação a seguir inicia um instantâneo de 8 GiB, usando o instantâneo `snap-123EXAMPLE1234567` como o instantâneo pai. O novo snapshot será um snapshot incremental do snapshot pai. O snapshot será movido para um estado de erro se não houver solicitações put ou complete feitas para o snapshot dentro do período limite especificado de `60` minutos. O token `550e8400-e29b-41d4-a716-446655440000` do cliente garante idempotência para a solicitação. Se o token do cliente for omitido, o AWS SDK gerará

automaticamente um para você. Para obter mais informações sobre idempotência, consulte Idempotência para API StartSnapshot .

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

O exemplo de resposta a seguir para a solicitação anterior mostra o ID do snapshot, o ID da conta da AWS , o status, o tamanho do volume em GiB e o tamanho dos blocos no snapshot. O snapshot é iniciado em estado pendente. Especifique o ID do snapshot em uma solicitação `PutSnapshotBlocks` subsequente para gravar dados no snapshot.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 929e6eb9-7183-405a-9502-5b7da37c1b18
Content-Type: application/json
Content-Length: 181
Date: Thu, 18 Jun 2020 04:07:29 GMT
Connection: keep-alive

{
    "BlockSize": 524288,
    "Description": null,
    "OwnerId": "138695307491",
    "Progress": null,
    "SnapshotId": "snap-052EXAMPLEc85d8dd",
    "StartTime": null,
    "Status": "pending",
    "Tags": null,
    "VolumeSize": 8
}
```

Inserir dados em um snapshot

AWS CLI

O comando de exemplo put-snapshot a seguir grava `524288` bytes de dados no índice de bloco `1000` no snapshot `snap-0aaEXAMPLEe306d62`. A soma de verificação `QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=` codificada pelo Base64 foi gerada com o uso do algoritmo SHA256. Os dados transmitidos ficam no arquivo `/tmp/data`.

```
aws ebs put-snapshot-block --snapshot-id snap-0aaEXAMPLEe306d62
 --block-index 1000 --data-length 524288 --block-data /tmp/data --
checksum QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= --checksum-algorithm SHA256
```

A resposta de exemplo a seguir para o comando anterior confirma o comprimento dos dados, a soma de verificação e o algoritmo de soma de verificação para os dados recebidos pelo serviço.

```
{
    "DataLength": "524288",
    "Checksum": "QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=",
    "ChecksumAlgorithm": "SHA256"
}
```

AWS API

O PutSnapshotexemplo a seguir grava `524288` bytes de dados `1000` no índice de blocos no snapshot`snap-052EXAMPLEc85d8dd`. A soma de verificação `QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=` codificada pelo Base64 foi gerada com o uso do algoritmo SHA256. Os dados são transmitidos no corpo da solicitação e são representados como *`BlockData`*no exemplo a seguir.

```
PUT /snapshots/snap-052EXAMPLEc85d8dd/blocks/1000 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-Data-Length: 524288
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T042215Z
X-Amz-Content-SHA256: UNSIGNED-PAYLOAD
Authorization: <Authentication parameter>
```

```
            BlockData
```

Veja a seguir a resposta de exemplo para a solicitação anterior, que confirma o comprimento dos dados, a soma de verificação e o algoritmo de soma de verificação para os dados recebidos pelo serviço.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 643ac797-7e0c-4ad0-8417-97b77b43c57b
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/json
Content-Length: 2
Date: Thu, 18 Jun 2020 04:22:12 GMT
Connection: keep-alive

{}
```

Concluir um snapshot

AWS CLI

O comando de exemplo complete-snapshot a seguir conclui o snapshot `snap-0aaEXAMPLEe306d62`. O comando especifica que 5 blocos foram gravados no snapshot. A soma de verificação `6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=` representa a soma de verificação para o conjunto completo de dados gravados em um snapshot. Para obter mais informações sobre somas de verificação, consulte Usar somas de verificação anteriormente neste guia.

```
aws ebs complete-snapshot --snapshot-id snap-0aaEXAMPLEe306d62 --changed-blocks-
count 5 --checksum 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= --checksum-
algorithm SHA256 --checksum-aggregation-method LINEAR
```

Veja a seguir um exemplo de resposta para o comando anterior.

```
{
    "Status": "pending"
}
```

AWS API

O CompleteSnapshotexemplo de solicitação a seguir conclui o snapshotsnap-052EXAMPLEc85d8dd. O comando especifica que 5 blocos foram gravados no snapshot. A soma de verificação 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= representa a soma de verificação para o conjunto completo de dados gravados em um snapshot.

```
POST /snapshots/completion/snap-052EXAMPLEc85d8dd HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-ChangedBlocksCount: 5
x-amz-Checksum: 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=
x-amz-Checksum-Algorithm: SHA256
x-amz-Checksum-Aggregation-Method: LINEAR
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T043158Z
Authorization: <Authentication parameter>
```

Veja a seguir um exemplo de resposta para a solicitação anterior.

```
HTTP/1.1 202 Accepted
x-amzn-RequestId: 06cba5b5-b731-49de-af40-80333ac3a117
Content-Type: application/json
Content-Length: 20
Date: Thu, 18 Jun 2020 04:31:50 GMT
Connection: keep-alive

{"Status":"pending"}
```

Usar criptografia

Quando você inicia um novo snapshot usando StartSnapshot, o status da criptografia depende dos valores que você especifica para Encrypted, KmsKeyArn e ParentSnapshotId e se sua AWS conta está habilitada para criptografia por padrão.

> **Note**
>
> - Talvez sejam necessárias permissões adicionais do IAM para uso das APIs diretas do EBS com criptografia. Para obter mais informações, consulte Permissões de uso AWS KMS keys.

- Se a criptografia do Amazon EBS estiver ativada por padrão em sua AWS conta, você não poderá criar snapshots não criptografados.
- Se a criptografia do Amazon EBS estiver habilitada por padrão em sua AWS conta, você não poderá iniciar um novo snapshot usando um snapshot principal não criptografado. Primeiro, será necessário criptografar o snapshot pai copiando-o. Para ter mais informações, consulte Copiar um snapshot do Amazon EBS..

Tópicos

Resultados de criptografia: snapshot pai não criptografado

A tabela a seguir descreve o resultado da criptografia para cada combinação possível de configurações ao especificar um snapshot pai não criptografado.

ParentSnapshotIdentificação	Criptografado	KmsKeyArn	Criptografia por padrão	Resultado
Não criptografado	Omitido	Omitido	Habilitado	Falha na solicitação com `ValidationException`.
			Desabilitado	O snapshot não está criptografado.
		Especificado	Habilitado	
			Desabilitado	
Não criptografado	Verdadeiro	Omitido	Habilitado	Falha na solicitação com `ValidationException`.
			Desabilitado	
		Especificado	Habilitado	

ParentSnapshotIdentificação	Criptografado	KmsKeyArn	Criptografia por padrão	Resultado
			Desabilitado	
Não criptografado	Falso	Omitido	Habilitado	Falha na solicitação com `ValidationException`.
			Desabilitado	
		Especificado	Habilitado	
			Desabilitado	

Resultados de criptografia: snapshot pai criptografado

A tabela a seguir descreve o resultado da criptografia para cada combinação possível de configurações ao especificar um snapshot pai criptografado.

ParentSnapshotIdentificação	Criptografado	KmsKeyArn	Criptografia por padrão	Resultado
Criptografado	Omitido	Omitido	Habilitado	O snapshot é criptografado usando a mesma chave do KMS do snapshot pai.
			Desabilitado	
		Especificado	Habilitado	Falha na solicitação com `ValidationException`.
			Desabilitado	
Criptografado	Verdadeiro	Omitido	Habilitado	Falha na solicitação com `ValidationException`.
			Desabilitado	
		Especificado	Habilitado	
			Desabilitado	

ParentSnapshotIdentificação	Criptografado	KmsKeyArn	Criptografia por padrão	Resultado
Criptografado	Falso	Omitido	Habilitado	Falha na solicitação com `ValidationException`.
			Desabilitado	
		Especificado	Habilitado	
			Desabilitado	

Resultados de criptografia: nenhum snapshot pai

As tabelas a seguir descrevem o resultado da criptografia para cada combinação possível de configurações ao não usar um snapshot pai.

ParentSnapshotIdentificação	Criptografado	KmsKeyArn	Criptografia por padrão	Resultado
Omitido	Verdadeiro	Omitido	Habilitado	O snapshot é criptografado usando a chave KMS padrão para sua conta. *
			Desabilitado	
		Especificado	Habilitado	O snapshot é criptografado usando a chave KMS especificada para KmsKey Arn.
			Desabilitado	
Omitido	Falso	Omitido	Habilitado	Falha na solicitação com `ValidationException`.
			Desabilitado	O snapshot não está criptografado.
		Especificado	Habilitado	Falha na solicitação com `ValidationException`.
			Desabilitado	

ParentSnapshotIdentificação	Criptografado	KmsKeyArn	Criptografia por padrão	Resultado
Omitido	Omitido	Omitido	Habilitado	O snapshot é criptografado usando a chave KMS padrão para sua conta. *
			Desabilitado	O snapshot não está criptografado.
		Especificado	Habilitado	O snapshot é criptografado usando a chave KMS especificada para KmsKey Arn.
			Desabilitado	

* Essa chave KMS padrão pode ser uma chave gerenciada pelo cliente ou a chave KMS AWS gerenciada padrão para a criptografia do Amazon EBS.

Usar a assinatura do Signature versão 4.

A versão 4 do Signature é o processo para adicionar informações de autenticação às AWS solicitações enviadas por HTTP. Por motivos de segurança, a maioria das solicitações AWS deve ser assinada com uma chave de acesso, que consiste em uma ID da chave de acesso e uma chave de acesso secreta. Essas duas chaves são comumente conhecidas como suas credenciais de segurança. Para obter informações sobre como obter credenciais para sua conta, consulte Credenciais de segurança da AWS.

Caso pretenda criar solicitações HTTP manualmente, é necessário aprender a assiná-las. Quando você usa o AWS Command Line Interface (AWS CLI) ou um dos AWS SDKs para fazer solicitações AWS, essas ferramentas assinam automaticamente as solicitações para você com a chave de acesso que você especifica ao configurar as ferramentas. Se você usar essas ferramentas, não precisará saber como assinar solicitações por si mesmo.

Para obter mais informações, consulte Solicitações de AWS API de assinatura no Guia do usuário do IAM.

Usar somas de verificação

A GetSnapshotBlock ação retorna dados que estão em um bloco de um instantâneo, e a PutSnapshotBlock ação adiciona dados a um bloco em um instantâneo. Os dados de bloco transmitidos não são assinados como parte do processo de assinatura do Signature versão 4. Como resultado, as somas de verificação são usadas para validar a integridade dos dados da seguinte forma:

- Quando você usa a GetSnapshotBlock ação, a resposta fornece uma soma de verificação SHA256 codificada em Base64 para os dados do bloco usando o cabeçalho X-AMZ-Checksum e o algoritmo de soma de verificação usando o cabeçalho X-AMZ-Checksum-Algorithm. Use a soma de verificação retornada para validar a integridade dos dados. Se a soma de verificação gerada não corresponder à que o Amazon EBS forneceu, considere os dados não válidos e tente enviar sua solicitação novamente.
- Ao usar a PutSnapshotBlock ação, sua solicitação deve fornecer uma soma de verificação SHA256 codificada em Base64 para os dados do bloco usando o cabeçalho X-AMZ-Checksum e o algoritmo de soma de verificação usando o cabeçalho X-AMZ-Checksum-Algorithm. A soma de verificação fornecida é validada com relação a uma soma de verificação gerada pelo Amazon EBS para validar a integridade dos dados. Se as somas de verificação não forem correspondentes, a solicitação falhará.
- Quando você usa a CompleteSnapshot ação, sua solicitação pode, opcionalmente, fornecer uma soma de verificação SHA256 agregada codificada em Base64 para o conjunto completo de dados adicionados ao snapshot. Forneça a soma de verificação usando o cabeçalho x-amz-Checksum, o algoritmo de soma de verificação usando o cabeçalho x-amz-Checksum-Algorithm e o método de agregação da soma de verificação usando o cabeçalho x-amz-Checksum-Aggregation-Method. Para gerar a soma de verificação agregada usando o método de agregação linear, organize as somas de verificação para cada bloco gravado na ordem crescente do índice do bloco, concatene-as de modo a formar uma única string e gere a soma de verificação em toda a string usando o algoritmo SHA256.

As somas de verificação nessas ações fazem parte do processo de assinatura do Signature versão 4.

Idempotência para API StartSnapshot

A idempotência garante que uma solicitação de API seja concluída apenas uma vez. Com uma solicitação idempotente, se a solicitação original for concluída com êxito, as novas tentativas subsequentes retornam o resultado da solicitação original bem-sucedida e não terão efeito adicional.

A StartSnapshotAPI oferece suporte à idempotência usando um token de cliente. Um token de cliente é uma string exclusiva que você especifica ao fazer uma solicitação de API. Se você tentar refazer uma solicitação de API com o mesmo token de cliente e os mesmos parâmetros de solicitação depois de ela ter sido concluída com êxito, o resultado da solicitação original será retornado. Se você tentar refazer uma solicitação com o mesmo token de cliente, mas alterar um ou mais parâmetros de solicitação, o erro `ConflictException` será retornado.

Se você não especificar seu próprio token de cliente, os AWS SDKs gerarão automaticamente um token de cliente para a solicitação, a fim de garantir que ela seja idempotente.

Um token de cliente pode ser qualquer cadeia de caracteres contendo até 64 caracteres ASCII. Não reutilize os mesmos tokens de cliente para solicitações diferentes.

Para fazer uma StartSnapshot solicitação idempotente com seu próprio token de cliente usando a API

Especifique o parâmetro de solicitação `ClientToken`.

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

Para fazer uma StartSnapshot solicitação idempotente com seu próprio token de cliente usando o AWS CLI

Especifique o parâmetro de solicitação `client-token`.

```
$ C:\> aws ebs start-snapshot --region us-east-2 --volume-size 8 --parent-
snapshot snap-123EXAMPLE1234567 --timeout 60 --client-token 550e8400-e29b-41d4-
a716-446655440000
```

Novas tentativas com erro

Os SDKs da AWS implementam uma lógica de novas tentativas automáticas para solicitações que retornam respostas de erro. É possível definir as configurações de novas tentativas para os SDKs da AWS . Para obter mais informações, consulte a documentação do SDK.

Você pode configurar a AWS CLI para fazer automaticamente novas tentativas para algumas solicitações com falha. Para obter mais informações sobre como configurar novas tentativas para o AWS CLI, consulte AWS CLI novas tentativas no Guia do AWS Command Line Interface usuário.

AAPI de consulta da AWS não oferece suporte à lógica de novas tentativas para solicitações com falha. Se você estiver usando solicitações HTTP ou HTTPS, deverá implementar a lógica de novas tentativas na aplicação do seu cliente.

A tabela a seguir mostra as possíveis respostas de erro da API. Alguns erros de API podem ser tentados novamente. A aplicação cliente deve sempre repetir solicitações com falha que recebam um erro que possa ser repetido.

Erro	Código de resposta	Descrição	Lançada por	Pode ser tentado novamente?
`InternalServerException`	500	A solicitação falhou devido a um problema na rede ou no AWS servidor.	Todas as APIs	Sim
`ThrottlingException`	400	O número de solicitações de API excedeu o limite máximo permitido do controle de utilização de	Todas as APIs	Sim

Erro	Código de resposta	Descrição	Lançada por	Pode ser tentado novamente?
		solicitações de API para a conta.		
`RequestThrottleException`	400	O número de solicitações de API excedeu o limite máximo permitido do controle de utilização de solicitações de API para o snapshot.	GetSnapshotBlock | PutSnapshotBlock	Sim
`ValidationException` com mensagem `"Failed to read block data”`	400	O bloco de dados fornecido não era legível.	PutSnapshotBloquear	Sim
`ValidationException` com qualquer outra mensagem	400	A sintaxe da solicitação está mal formada ou a entrada não satisfaz as restrições especificadas pelo AWS service (Serviço da AWS).	Todas as APIs	Não

Erro	Código de resposta	Descrição	Lançada por	Pode ser tentado novamente?
`ResourceNotFoundException`	404	A ID de snapshot especificada não existe.	Todas as APIs	Não
`ConflictException`	409	O token de cliente especificado foi usado anteriormente em uma solicitação semelhante e que tinha parâmetros de solicitação diferentes. Para ter mais informações, consulte Idempotência para API StartSnapshot .	StartSnapshot	Não
`AccessDeniedException`	403	Você não tem a permissão para realizar a operação solicitada.	Todas as APIs	Não

Erro	Código de resposta	Descrição	Lançada por	Pode ser tentado novamente?
`ServiceQuotaExceededException`	402	A solicitação falhou porque o atendimento da solicitação excederia uma ou mais service quotas dependentes para sua conta.	Todas as APIs	Não
`InvalidSignatureException`	403	A assinatura de autorização da solicitação expirou. Você pode repetir a solicitação somente depois de atualizar a assinatura de autorização.	Todas as APIs	Não

Otimizar a performance

É possível executar solicitações de API simultaneamente. Supondo que a PutSnapshotBlock latência seja de 100 ms, um thread pode processar 10 solicitações em um segundo. Além disso, supondo que a aplicação do cliente crie vários threads e conexões (por exemplo, 100 conexões), ela poderá fazer 1000 (10 * 100) solicitações por segundo no total. Isso corresponde a uma throughput de cerca de 500 MB por segundo.

A lista a seguir contém alguns itens a serem observados na aplicação:

- Cada thread está usando uma conexão distinta? Se as conexões são limitadas na aplicação, vários threads aguardarão a disponibilidade da conexão e você perceberá uma throughput menor.

- Há algum tempo de espera na aplicação entre duas solicitações put? Isso reduzirá a throughput efetiva de um thread.
- O limite de largura de banda na instância — Se a largura de banda na instância for compartilhada por outros aplicativos, isso poderá limitar a taxa de transferência disponível para solicitações. PutSnapshotBlock

Para evitar gargalos, certifique-se de observar outras workloads que podem estar em execução na conta. Você também deve criar mecanismos de repetição nos fluxos de trabalho de APIs diretas do EBS para lidar com o controle de utilização, os tempos limite e a indisponibilidade do serviço.

Revise as Service Quotas das APIs diretas do EBS para determinar o número máximo de solicitações de API que é possível executar por segundo. Para obter mais informações, consulte Endpoints e cotas do Amazon Elastic Block Store na Referência geral da AWS .

Endpoints de serviço de APIs diretas do EBS

Um endpoint é uma URL que serve como ponto de entrada para um serviço AWS web. As APIs diretas do EBS são compatíveis com os seguintes tipos de endpoint:

- Endpoints IPv4
- Endpoints de pilha dupla que são compatíveis com IPv4 e IPv6
- Endpoints do FIPS

Ao fazer uma solicitação, você pode especificar o endpoint e a região a serem usados. Se você não especificar um endpoint, o endpoint IPv4 será usado por padrão. Para usar outro tipo de endpoint, você deve especificá-lo em sua solicitação. Para obter exemplos de como fazer isso, consulte Especificar endpoints.

Para obter mais informações sobre regiões, consulte Regiões e zonas de disponibilidade no Guia do usuário do Amazon EC2. Para obter uma lista de endpoints para APIs diretas do EBS, consulte Endpoints para as APIs diretas do EBS no Referência geral da Amazon Web Services.

Tópicos

- Especificar endpoints

Endpoints IPv4

Endpoints IPv4 só são compatíveis com tráfego IPv4. Os endpoints IPv4 estão disponíveis em todas as regiões.

As APIs diretas do EBS oferecem suporte somente a endpoints IPv4 regionais que você pode usar para fazer suas solicitações. Você deve especificar a região como parte do nome do endpoint. Os nomes dos endpoints usam a seguinte convenção de nomenclatura:

- `ebs.`*`region`*`.amazonaws.com`

Por exemplo, para direcionar suas solicitações para o endpoint `us-east-2` IPv4, você deve especificar `ebs.us-east-2.amazonaws.com` como endpoint. Para obter uma lista de endpoints para APIs diretas do EBS, consulte Endpoints para as APIs diretas do EBS no Referência geral da Amazon Web Services.

Definição de preço

Você não é cobrado por dados transferidos diretamente entre APIs diretas do EBS e instâncias do Amazon EC2 usando um endpoint IPv4 na mesma região. No entanto, se houver serviços intermediários, como AWS PrivateLink endpoints, NAT Gateway ou Amazon VPC Transit Gateways, você será cobrado pelos custos associados.

Endpoints de pilha dupla (IPv4 e IPv6)

Endpoints de pilha dupla são compatíveis com tráfego IPv4 e IPv6. Os endpoints de pilha dupla estão disponíveis em todas as regiões.

Para usar o IPv6, você deve usar um endpoint de pilha dupla. Quando você realiza uma solicitação para um endpoint de pilha dupla, o URL do endpoint decide por um endereço IPv6 ou IPv4, dependendo do protocolo usado pela rede e pelo cliente.

As APIs diretas do EBS são compatíveis apenas com endpoints de pilha dupla regionais, o que significa que você deve especificar a região como parte do nome do endpoint. Os nomes de endpoints de pilha dupla usam a seguinte convenção de nomenclatura:

- `ebs.`*`region`*`.api.aws`

Por exemplo, o nome do endpoint de pilha dupla para a região `eu-west-1` é `ebs.eu-west-1.api.aws`. Para obter uma lista de endpoints para APIs diretas do EBS, consulte Endpoints para as APIs diretas do EBS no Referência geral da Amazon Web Services.

Definição de preço

Você não é cobrado por dados transferidos diretamente entre APIs diretas do EBS e instâncias do Amazon EC2 usando um endpoint de pilha dupla na mesma região. No entanto, se houver serviços intermediários, como AWS PrivateLink endpoints, NAT Gateway ou Amazon VPC Transit Gateways, você será cobrado pelos custos associados.

Endpoints do FIPS

As APIs diretas do EBS fornecem endpoints IPv4 e de pilha dupla (IPv4 e IPv6) validados pelo FIPS para as seguintes regiões:

- `us-east-1` - Leste dos EUA (Norte da Virgínia):
- `us-east-2` - Leste dos EUA (Ohio)
- `us-west-1` - Oeste dos EUA (N. da Califórnia)
- `us-west-2` - Oeste dos EUA (Oregon):
- `ca-central-1` - Canadá (Central)

Endpoints FIPS IPv4 usam a seguinte convenção de nomenclatura: `ebs-fips.`*`region`*`.amazonaws.com`. Por exemplo, o endpoint FIPS IPv4 para `us-east-1` é `ebs-fips.us-east-1.amazonaws.com`.

Endpoints FIPS de pilha dupla usam a seguinte convenção de nomenclatura: `ebs-fips.`*`region`*`.api.aws`. Por exemplo, o endpoint FIPS de pulha dupla para `us-east-1` é `ebs-fips.us-east-1.api.aws`.

Para obter mais informações sobre endpoints do FIPS, consulte Endpoints do FIPS no Referência geral da Amazon Web Services.

Especificar endpoints

Esta seção fornece alguns exemplos de como especificar um endpoint ao fazer uma solicitação.

AWS CLI

Os exemplos a seguir mostram como especificar um endpoint para a região deus-east-2 usando o AWS CLI.

- Pilha dupla

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.us-east-2.api.aws
```

- IPv4

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.us-east-2.amazonaws.com
```

AWS SDK for Java 2.x

Os exemplos a seguir mostram como especificar um endpoint para a região deus-east-2 usando o AWS SDK for Java 2.x.

- Pilha dupla

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.api.aws", "us-
east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

- IPv4

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.amazonaws.com",
 "us-east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

AWS SDK for Go

Os exemplos a seguir mostram como especificar um endpoint para a região deus-east-2 usando o AWS SDK for Go.

- Pilha dupla

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast1RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.api.aws")
})
```

- IPv4

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast1RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.amazonaws.com")
})
```

Preços de APIs diretas do EBS

Tópicos

- Preço de APIs
- Custos de rede

Preço de APIs

O preço pago por uso das APIs diretas do EBS depende das solicitações feitas. Para obter mais informações, consulte Definição de preço do Amazon EBS.

- ListChangedOs blocos e as ListSnapshotBlocks APIs são cobrados por solicitação. Por exemplo, se você fizer 100.000 solicitações de ListSnapshotBlocks API em uma região que cobra 0,0006 USD por 1.000 solicitações, você será cobrado 0,06 USD (0,0006 USD por 1.000 solicitações x 100).

- GetSnapshotO bloco é cobrado por bloco devolvido. Por exemplo, se você fizer 100.000 solicitações de GetSnapshotBlock API em uma região que cobra 0,003 USD por 1.000 blocos retornados, você será cobrado 0,30 USD (0,003 USD por 1.000 blocos retornados x 100).
- PutSnapshotO bloco é cobrado por bloco gravado. Por exemplo, se você fizer 100.000 solicitações de PutSnapshotBlock API em uma região que cobra 0,006 USD por 1.000 blocos gravados, você será cobrado 0,60 USD (0,006 USD por 1.000 blocos gravados x 100).

Custos de rede

Custos de transferência de dados

Os dados transferidos diretamente entre as APIs diretas do EBS e as instâncias do Amazon EC2 na AWS mesma região são gratuitos ao usar endpoints não FIPS. Para obter mais informações, consulte Endpoints de serviço da AWS. Se outros AWS serviços estiverem no caminho de sua transferência de dados, você será cobrado pelos custos de processamento de dados associados. Esses serviços incluem, mas não estão limitados a, PrivateLink endpoints, NAT Gateway e Transit Gateway.

Endpoints de interface com VPC

Se você estiver usando APIs diretas do EBS de instâncias AWS Lambda ou funções do Amazon EC2 em sub-redes privadas, você pode usar endpoints de interface VPC, em vez de usar gateways NAT, para reduzir os custos de transferência de dados da rede. Para ter mais informações, consulte Uso de APIs diretas do EBS e endpoints da VPC de interface.

Uso de APIs diretas do EBS e endpoints da VPC de interface

É possível estabelecer uma conexão privada entre a VPC e as APIs diretas do EBS criando um endpoint da VPC de interface, com tecnologia AWS PrivateLink. É possível acessar APIs diretas do EBS como se estivesse em sua VPC, sem usar um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão AWS Direct Connect . As instâncias na VPC não precisam de endereços IP públicos para a comunicação com APIs diretas do EBS.

Criaremos uma interface de rede de endpoint em cada sub-rede que você habilitar para o endpoint de interface.

Para obter mais informações, consulte Acesso Serviços da AWS por meio AWS PrivateLink do AWS PrivateLink Guia.

Considerações para endpoints da VPC de APIs diretas do EBS

Antes de configurar um endpoint da VPC de interface para APIs diretas do EBS, analise as considerações no Guia do AWS PrivateLink .

Por padrão, o acesso total às APIs diretas do EBS é permitido pelo endpoint. Você pode controlar o acesso ao endpoint da interface usando as políticas de endpoint da VPC. Você pode anexar uma política de endpoint ao seu VPC endpoint que controla o acesso às APIs diretas do EBS. Essa política especifica as seguintes informações:

- O principal que pode realizar ações.
- As ações que podem ser executadas.
- Os recursos nos quais as ações podem ser executadas.

Para obter mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Veja a seguir um exemplo de uma política de endpoint para APIs diretas do EBS. Quando anexada a um endpoint, essa política concede acesso a todas as ações diretas das APIs do EBS em todos os recursos, exceto snapshots marcados com chave e valor. `Environment` `Test`

```
{
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Environment": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*"
        }
```

```
    ]
}
```

Criar um endpoint da VPC de interface para APIs diretas do EBS

É possível criar um endpoint da VPC para APIs diretas do EBS usando o console da Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Create a VPC endpoint (Criar um endpoint da VPC) no Guia do AWS PrivateLink .

Criar um endpoint da VPC para APIs diretas do EBS usando o seguinte nome de serviço:

- `com.amazonaws.region.ebs`

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para as APIs diretas do EBS usando seu nome DNS padrão para a região, por exemplo, `ebs.us-east-1.amazonaws.com`.

Registre chamadas de API para APIs diretas do EBS com AWS CloudTrail

O serviço de APIs diretas do EBS está integrado a. AWS CloudTrail CloudTrail é um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço. CloudTrail captura todas as chamadas de API realizadas nas APIs diretas do EBS como eventos. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon Simple Storage Service (Amazon S3). Se você não configurar uma trilha, ainda poderá ver os eventos de gerenciamento mais recentes no CloudTrail console no Histórico de eventos. Os eventos de dados não são capturados no histórico de eventos. Você pode usar as informações coletadas por CloudTrail para determinar a solicitação feita às APIs diretas do EBS, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações sobre as APIs diretas do EBS em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade de evento suportada ocorre nas APIs diretas do EBS, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e

baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo de eventos em sua AWS conta, incluindo eventos para APIs diretas do EBS, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Ações da API com suporte

Para APIs diretas do EBS, você pode usar CloudTrail para registrar dois tipos de eventos:

- Eventos de gerenciamento — Os eventos de gerenciamento fornecem visibilidade das operações de gerenciamento que são realizadas em instantâneos em sua AWS conta. Por padrão, as seguintes ações de API são registradas como eventos de gerenciamento em trilhas:
  - StartSnapshot
  - CompleteSnapshot

  Para obter mais informações sobre eventos de gerenciamento de registros, consulte Registrar eventos de gerenciamento para trilhas no Guia CloudTrail do usuário.
- Eventos de dados: estes eventos fornecem visibilidade nas operações do snapshot executadas no snapshot ou dentro de um snapshot. Opcionalmente, as seguintes ações de API podem ser registradas como eventos de dados em trilhas:
  - ListSnapshotBlocos
  - ListChangedBlocos
  - GetSnapshotBlock
  - PutSnapshotBloquear

Eventos de dados não são registrados por padrão quando você cria uma trilha. É possível usar apenas seletores de eventos avançados para registrar eventos de dados em chamadas diretas de API do EBS. Para obter mais informações, consulte Registro de eventos de dados para trilhas no Guia CloudTrail do usuário.

> **Note**
>
> Se você realizar uma ação em um snapshot compartilhado com você, os eventos de dados não serão enviados para a AWS conta proprietária do snapshot.

Informações de identidade

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o CloudTrail usuário IdentityElement.

Compreender as entradas do arquivo de log de APIs diretas do EBS

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Veja a seguir exemplos de entradas de CloudTrail registro.

StartSnapshot

```
{
    "eventVersion": "1.05",
```

```
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:27:26Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "StartSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "volumeSize": 8,
        "clientToken": "token",
        "encrypted": true
    },
    "responseElements": {
        "snapshotId": "snap-123456789012",
        "ownerId": "123456789012",
        "status": "pending",
        "startTime": "Jul 3, 2020 11:27:26 PM",
        "volumeSize": 8,
        "blockSize": 524288,
        "kmsKeyArn": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

CompleteSnapshot

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:28:24Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "CompleteSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "snapshotId": "snap-123456789012",
        "changedBlocksCount": 5
    },
    "responseElements": {
        "status": "completed"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

ListSnapshotBlocks

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-03T00:32:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListSnapshotBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "maxResults": 100,
```

```
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example6-0e12-4aa9-b923-1555eexample",
    "eventID": "example4-218b-4f69-a9e0-2357dexample",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

ListChangedBlocks

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:11:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListChangedBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
```

```
        "firstSnapshotId": "snap-abcdef01234567890",
        "secondSnapshotId": "snap-9876543210abcdef0",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example0-f4cb-4d64-8d84-72e1bexample",
    "eventID": "example3-fac4-4a78-8ebb-3e9d3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        },
       {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-9876543210abcdef0"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

GetSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
```

```
    },
    "eventTime": "2021-06-02T20:43:05Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "GetSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "blockToken": "EXAMPLEiL5E3pMPFpaDWjExM2/mnSKh1mQfcbjwe2mM7EwhrgCdPAEXAMPLE"
    },
    "responseElements": null,
    "requestID": "examplea-6eca-4964-abfd-fd9f0example",
    "eventID": "example6-4048-4365-a275-42e94example",
    "readOnly": true,
    "resources": [
        {
          "accountId": "123456789012",
          "type": "AWS::EC2::Snapshot",
          "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

PutSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:09:17Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "PutSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "dataLength": 524288,
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "responseElements": {
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "requestID": "example3-d5e0-4167-8ee8-50845example",
    "eventID": "example8-4d9a-4aad-b71d-bb31fexample",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

Perguntas frequentes

Um snapshot pode ser acessado usando as APIs diretas do EBS se tiver um status pendente?

Não. O snapshot só poderá ser acessado se tiver um status concluído.

Os índices de bloco são retornados pelas APIs diretas do EBS em ordem numérica?

Sim. Os índices de bloco retornados são exclusivos e em ordem numérica.

Posso enviar uma solicitação com um valor de MaxResults parâmetro abaixo de 100?

Não. O valor mínimo do MaxResult parâmetro que você pode usar é 100. Se você enviar uma solicitação com um valor de MaxResult parâmetro inferior a 100 e houver mais de 100 blocos no snapshot, a API retornará pelo menos 100 resultados.

Posso executar solicitações de API simultaneamente?

É possível executar solicitações de API simultaneamente. Para evitar gargalos, certifique-se de observar outras workloads que podem estar em execução na conta. Você também deve criar mecanismos de repetição nos fluxos de trabalho de APIs diretas do EBS para lidar com o controle de utilização, os tempos limite e a indisponibilidade do serviço. Para obter mais informações, consulte Otimizar a performance.

Revise as Service Quotas das APIs diretas do EBS para determinar o número de solicitações de API que é possível executar por segundo. Para obter mais informações, consulte Endpoints e cotas do Amazon Elastic Block Store na Referência geral da AWS .

Ao executar a ListChangedBlocks ação, é possível obter uma resposta vazia mesmo que haja blocos no instantâneo?

Sim. Se os blocos alterados forem escassos no snapshot, a resposta poderá ser vazia, mas a API retornará um valor de token de próxima página. Use o valor de token de próxima página para continuar na próxima página de resultados. É possível confirmar que atingiu a última página de resultados quando a API retornar um valor nulo de token de próxima página.

Se o NextToken parâmetro for especificado junto com um StartingBlockIndex parâmetro, qual dos dois será usado?

O NextToken é usado e o StartingBlockIndex é ignorado.

Por quanto tempo os tokens de bloco e os próximos tokens são válidos?

Os tokens de bloco são válidos por sete dias e os próximos tokens são válidos por 60 minutos.

Há suporte para snapshots criptografados?

Sim. Os snapshots criptografados podem ser acessados usando as APIs diretas do EBS.

Para acessar um instantâneo criptografado, o usuário deve ter acesso à chave KMS usada para criptografar o instantâneo e à ação de descriptografia. AWS KMS Consulte a Permissões do IAM para APIs diretas do EBS seção anterior neste guia para ver a AWS KMS política a ser atribuída a um usuário.

Há suporte para snapshots públicos?

Snapshots públicos não são compatíveis.

Há suporte para snapshots locais do Amazon EBS no Outposts?

Não há suporte para snapshots locais do Amazon EBS no Outposts.

A listagem de blocos do snapshot retorna todos os índices e os tokens de bloco em um snapshot, ou somente aqueles que têm dados gravados neles?

Ela retorna somente os índices e os tokens de bloco que têm dados gravados neles.

Posso obter um histórico das chamadas de API realizadas pelas APIs diretas do EBS na minha conta para fins de análise de segurança ou solução de problemas operacionais?

Sim. Para receber um histórico de chamadas de API de APIs diretas do EBS feitas em sua conta, ative o AWS CloudTrail no AWS Management Console. Para ter mais informações, consulte Registre chamadas de API para APIs diretas do EBS com AWS CloudTrail.

Segurança no Amazon Elastic Block Store

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de data centers e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: AWS é responsável pela proteção da infraestrutura que executaAWS produtos da Nuvem AWS na AWS. A também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos AWSProgramas de conformidade. Para conhecer os programas de conformidade que se aplicam ao Amazon Elastic Block Store, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na 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 empresa e as leis e regulamentos aplicáveis.

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

Tópicos

Proteção de dados no Amazon Elastic Block Store

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no Amazon Elastic Block Store. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle

sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a publicação no blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

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 IAM Identity Center ou o AWS Identity and Access Management (IAM). Dessa maneira, 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 SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Amazon EBS ou outros Serviços da AWS usando o console, a API, a AWS CLI ou os AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Tópicos

- Gerenciamento de chaves do KMS

Segurança de dados do Amazon EBS

Os volumes do Amazon EBS são apresentados a você como dispositivos de bloco brutos e não formatados. Eles são dispositivos lógicos criados na infraestrutura do EBS, e o serviço Amazon EBS garante que os dispositivos estejam logicamente vazios (ou seja, os blocos brutos são zerados ou contêm dados pseudorrandomizados criptograficamente) antes de qualquer uso ou reutilização por um cliente.

Se você tiver procedimentos que exigem que todos os dados sejam apagados usando um método específico, após ou antes do uso (ou ambos), como aqueles detalhados em DoD 5220,22-M (Manual Operacional do Programa Nacional de Segurança Industrial) ou em NIST 800-88 (Diretrizes para higienização de mídia), será possível fazer isso no Amazon EBS. Essa atividade em nível de bloco será refletida na mídia de armazenamento subjacente dentro do serviço do Amazon EBS.

Criptografia de dados em repouso e em trânsito

A criptografia do Amazon EBS é uma solução de criptografia que permite criptografar seus volumes e snapshots do Amazon EBS usando chaves criptográficas do AWS Key Management Service. As operações de criptografia do EBS ocorrem nos servidores que hospedam as instâncias do Amazon EC2, garantindo a segurança dos dados em repouso e dos dados em trânsito entre uma instância e seu volume anexado e quaisquer snapshots subsequentes. Para obter mais informações, consulte Criptografia do Amazon EBS.

Gerenciamento de chaves do KMS

Ao criar um volume do Amazon EBS criptografado, você especifica uma chave do AWS Key Management Service. Por padrão, o Amazon EBS usa a chave do KMS gerenciada pela AWS para o Amazon EBS na sua conta e região (`aws/ebs`). No entanto, é possível especificar uma chave do KMS gerenciada pelo cliente que você cria e gerencia. Usar uma chave do KMS gerenciada pelo cliente oferece a você mais flexibilidade, incluindo a capacidade de criar, alternar e desabilitar chaves do KMS.

Para usar uma chave do KMS gerenciada pelo cliente, você deve conceder aos usuários permissão para usar a chave do KMS. Para obter mais informações, consulte Permissões para usuário.

> **Important**
>
> O Amazon EBS oferece suporte somente a chaves do KMS simétricas. Não é possível usar chaves do KMS assimétricas para criptografar volumes e snapshots do Amazon EBS. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Como identificar chaves do KMS assimétricas.

Para cada volume, o Amazon EBS pede ao AWS KMS para gerar uma chave de dados exclusiva criptografada sob a chave do KMS que você especifica. O Amazon EBS armazena a chave de dados criptografada com o volume. Em seguida, quando você anexa o volume a uma instância do Amazon EC2, o Amazon EBS chama o AWS KMS para descriptografar a chave de dados. O Amazon EBS usa a chave de dados em texto simples na memória do hipervisor para criptografar toda a E/S no volume. Para obter mais informações, consulte Como funciona a criptografia do EBS.

Gerenciamento de identidade e acesso para Amazon Elastic Block Store

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (iniciar sessão) e autorizado (receber permissões) para utilizar os recursos do Amazon EBS. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

Público

A forma de usar o AWS Identity and Access Management (IAM) varia em função do trabalho realizado no Amazon EBS.

Usuário do serviço: se você usa o serviço do Amazon EBS para trabalhar, o administrador fornecerá as credenciais e as permissões necessárias. À medida que você usar mais recursos do Amazon EBS para trabalhar, poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Caso não consiga acessar um recurso no Amazon EBS, consulte Solução de problemas de identidade e acesso do Amazon EBS.

Administrador do serviço: se você for o responsável pelos recursos do Amazon EBS em sua empresa, provavelmente terá acesso total ao Amazon EBS. Cabe a você determinar quais funcionalidades e recursos do Amazon EBS os usuários do serviço deverão acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Amazon EBS, consulte Como o Amazon Elastic Block Store funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez deseje saber detalhes sobre como escrever políticas para gerenciar o acesso ao Amazon EBS. Para visualizar exemplos de políticas baseadas em identidade do Amazon EBS que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o Amazon Elastic Block Store.

Autenticando com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como um usuário do IAM ou assumindo um perfil do IAM.

Você pode fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center Os usuários do IAM Identity Center, a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no AWS Management Console ou no portal de acesso da AWS dependendo do tipo de usuário que você é. Para obter mais informações sobre como fazer login na AWS,

consulte How to sign in to your Conta da AWS (Como fazer login na conta da) no Guia do usuário do Início de Sessão da AWS.

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface da linha de comando (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinar solicitações de API da AWS no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça mais informações de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário. Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os recursos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web, o AWS Directory Service, o diretório do Centro de Identidade ou qualquer usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem os perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no Centro de Identidade do IAM ou se conectar e sincronizar com

um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. Para obter mais informações sobre o Centro de Identidade do IAM, consulte "O que é o Centro de Identidade do IAM?" no Guia do usuário do AWS IAM Identity Center.

Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de uma função) no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ela é semelhante a um usuário do IAM, mas não está associada a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais

informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário do AWS IAM Identity Center.

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar um perfil como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
  - Perfil vinculada a serviço: um perfil vinculado a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação

em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculadas ao serviço.

- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-lo para todas as aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define as respectivas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfis do AWS Management Console, da AWS CLI ou da API da AWS.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como um usuário do IAM, grupo de usuários ou função do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de política do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS aceita tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cada Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte Como os SCPs funcionam no Guia do usuário do AWS Organizations.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliaçãode políticas no Guia do usuário do IAM.

Como o Amazon Elastic Block Store funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Amazon EBS, saiba quais recursos do IAM estão disponíveis para uso com o Amazon EBS.

Recursos do IAM que você pode usar com o Amazon Elastic Block Store

Recurso do IAM	Suporte ao Amazon EBS
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Perfis vinculados ao serviço	Não

Para obter uma visão geral de como o Amazon EBS e outros serviços da AWS funcionam com a maioria dos recursos do IAM, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade do Amazon EBS

É compatível com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. ‘Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para o Amazon EBS

Para visualizar exemplos de políticas baseadas em identidade do Amazon EBS, consulte Exemplos de políticas baseadas em identidade para o Amazon Elastic Block Store.

Políticas baseadas em recursos no Amazon EBS

Oferece suporte a políticas baseadas em recursos	Não

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar um principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o recurso estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal

(usuário ou função) permissão para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a um principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações de políticas para o Amazon EBS

Oferece suporte a ações de políticas	Sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para visualizar uma lista de ações do Amazon EBS, consulte Ações, recursos e chaves de condição na Referência de autorização do serviço.

As ações de política no Amazon EBS usam o seguinte prefixo antes da ação:

```
ec2
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
  "ec2:action1",
  "ec2;:action2"
]
```

Para visualizar exemplos de políticas baseadas em identidade do Amazon EBS, consulte Exemplos de políticas baseadas em identidade para o Amazon Elastic Block Store.

Recursos de políticas para o Amazon EBS

Oferece suporte a recursos de políticas	Sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recursos do Amazon EBS e seus ARNs, consulte Recursos definidos pelo Amazon Elastic Block Store na Referência de autorização do serviço. Para saber com quais ações é possível especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon Elastic Block Store.

Algumas ações da API do Amazon EBS oferecem suporte a vários recursos. Para especificar vários recursos em uma única instrução, separe os ARNs com vírgulas. Por exemplo, `DescribeVolumes` tem acesso a vol-01234567890abcdef e vol-09876543210fedcba, portanto, uma entidade principal deve ter permissões para acessar os dois recursos.

```
"Resource": [
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-01234567890abcdef",
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-09876543210fedcba"
]
```

Chaves de condição de política para o Amazon EBS

Compatível com chaves de condição de política específicas do serviço	Sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as AWS chaves de condição globais da , consulte AWSChaves de contexto de condição globais da no Guia do usuário do IAM.

Por exemplo, a condição a seguir permitirá que a entidade principal execute uma ação em um volume somente se o tipo de volume for `gp2`.

```
"Condition":{
  "StringLikeIfExists":{
    "ec2:VolumeType":"gp2"
  }
}
```

Para visualizar uma lista de chaves de condição do Amazon EBS, consulte Ações, recursos e chaves de condição na Referência de autorização do serviço. Para saber com quais ações e recursos você pode usar a chave de condição, consulte Ações definidas pelo Amazon Elastic Block Store.

ACLs no Amazon EBS

Oferece suporte a ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com o Amazon EBS

Oferece suporte a ABAC (tags em políticas)	Parcial

O controle de acesso baseado em atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos recursos da AWS. A marcação de entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o Amazon EBS

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se faz login no AWS Management Console usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para uma função (console) no Guia do usuário do IAM.

Você pode criar credenciais temporárias manualmente usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidades principais entre serviços para o Amazon EBS

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou um perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Perfis de serviço para o Amazon EBS

Oferece suporte a perfis de serviço	Sim

O perfil de serviço é um perfil do IAMhttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte

Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

> **Warning**
>
> A alteração das permissões de um perfil de serviço pode interromper a funcionalidade do Amazon EBS. Edite perfis de serviço somente quando o Amazon EBS fornecer orientações para fazê-lo.

Perfis vinculados ao serviço para o Amazon EBS

Oferece suporte a perfis vinculados ao serviço	Não

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir a função de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte Serviços do AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço.

Exemplos de políticas baseadas em identidade para o Amazon Elastic Block Store

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Amazon EBS. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API AWS. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recurso definidos pelo Amazon EBS, por exemplo, o formato dos ARNs para cada um dos tipos de recurso, consulte Ações, recursos e chaves de condição do Amazon Elastic Block Store na Referência de autorização do serviço.

Tópicos

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Amazon EBS em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition no Manual do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar o console do Amazon EBS

Para acessar o console do Amazon Elastic Block Store, é necessário ter um conjunto mínimo de permissões. Essas permissões devem permitir listar e visualizar detalhes sobre os recursos do Amazon EBS em sua Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que os usuários e as funções ainda possam usar o console do Amazon EBS, anexe também a política `ConsoleAccess` ou `ReadOnly` gerenciada pela AWS às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a AWS API.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Trabalhar com volumes

Exemplos

- Exemplo: anexar e desanexar volumes
- Exemplo: criar um volume
- Exemplo: criar um volume com tags
- Exemplo: trabalhar com volumes usando o console do Amazon EC2

Exemplo: anexar e desanexar volumes

Quando uma ação da API exige que um chamador especifique vários recursos, crie uma declaração de política que permita que os usuários acessem todos os recursos necessários. Se você precisar usar um elemento `Condition` com um ou mais desses recursos, deverá criar várias declarações conforme mostrado neste exemplo.

As políticas a seguir permitem que os usuários anexem volumes com a tag "`volume_user=`iam-user-name" a instâncias com a tag "`department=dev`" e desanexem esses volumes dessas instâncias. Se você anexar essa política a um grupo do IAM, a variável da política `aws:username` fornecerá a cada usuário no grupo permissão para anexar e desanexar volumes das instâncias com uma tag chamada `volume_user` que tem o nome do usuário como um valor.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "dev"
        }
      }
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/volume_user": "${aws:username}"
        }
      }
   }
```

```
  ]
}
```

Exemplo: criar um volume

A política a seguir permite que os usuários usem a ação da API CreateVolume. O usuário terá permissão para criar um volume somente se o volume for criptografado e se seu tamanho for menor que 20 GiB.

```
{
  "Version": "2012-10-17",
  "Statement": [
         {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition":{
         "NumericLessThan": {
             "ec2:VolumeSize" : "20"
          },
          "Bool":{
              "ec2:Encrypted" : "true"
          }
       }
    }
  ]
}
```

Exemplo: criar um volume com tags

As política a seguir inclui a chave de condição `aws:RequestTag` que requer que os usuários marquem todos os volumes que criarem com as tags `costcenter=115` e `stack=prod`. Se os usuários não passarem essas tags específicas ou não especificarem nenhuma tag, haverá talha na solicitação.

Para ações de criação de recursos que aplicam tags, os usuários também devem ter permissões para usar a ação `CreateTags`. A segunda declaração usa a chave de condição `ec2:CreateAction` para permitir que os usuários criem tags somente no contexto de `CreateVolume`. Os usuários não podem marcar volumes existentes ou quaisquer outros recursos.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Sid": "AllowCreateTaggedVolumes",
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
         }
       }
     },
     {
       "Effect": "Allow",
       "Action": [
         "ec2:CreateTags"
       ],
       "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
       "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "CreateVolume"
        }
      }
    }
  ]
}
```

A política a seguir permite que os usuários criem um volume sem precisar especificar tags. A ação `CreateTags` só será avaliada se as tags forem especificadas na solicitação `CreateVolume`. Se os usuários especificam tags, a tag deverá ser `purpose=test`. Nenhuma outra tag é permitida na solicitação.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "CreateVolume"
          },
         "ForAllValues:StringEquals": {
             "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Exemplo: trabalhar com volumes usando o console do Amazon EC2

A política a seguir concede aos usuários permissão para visualizar e criar volumes, e para anexar e desanexar volumes em instâncias específicas usando o console do Amazon EC2.

Os usuários podem anexar um volume às instâncias que tenham a tag "`purpose=test`" e também desanexar volumes dessas instâncias. Para anexar um volume usando o console do Amazon EC2, é útil que os usuários tenham permissão para usar a ação `ec2:DescribeInstances`, pois isso permite que eles selecionem uma instância de uma lista pré-preenchida na caixa de diálogo Attach Volume (Anexar volume). No entanto, isso também permite que os usuários visualizem todas as instâncias na página Instances no console, portanto, é possível omitir essa ação.

Na primeira instrução, a ação `ec2:DescribeAvailabilityZones` é necessária para garantir que um usuário possa selecionar uma zona de disponibilidade ao criar um volume.

Os usuários não podem marcar os volumes que criam (durante ou após a criação do volume).

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

```
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateVolume",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/purpose": "test"
        }
     }
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:volume/*"
   }
   ]
}
```

Trabalhar com snapshots

Veja a seguir exemplos de políticas para `CreateSnapshot` (snapshot point-in-time de um volume do EBS) e `CreateSnapshots` (snapshots de vários volumes).

Exemplos

- Exemplo: criar um snapshot
- Exemplo: criar snapshots
- Exemplo: criar um snapshot com tags
- Exemplo: criar snapshots de vários volume com etiquetas

- Exemplo: Copiar snapshots
- Exemplo: modificar configurações de permissão para snapshots

Exemplo: criar um snapshot

A política a seguir permite que os clientes usem a ação da API CreateSnapshot. O cliente poderá criar snapshots somente se o volume for criptografado e se seu tamanho for menor que 20 GiB.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "NumericLessThan":{
               "ec2:VolumeSize":"20"
            },
            "Bool":{
               "ec2:Encrypted":"true"
            }
         }
      }
   ]
}
```

Exemplo: criar snapshots

A política a seguir permite que os clientes usem a ação da API CreateSnapshots. O cliente só poderá criar snapshots se todos os volumes da instância forem do tipo GP2.

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

```
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*"
   ]
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:volume/*",
         "Condition":{
            "StringLikeIfExists":{
               "ec2:VolumeType":"gp2"
             }
     }

      }
   ]
}
```

Exemplo: criar um snapshot com tags

A política a seguir inclui a chave de condição `aws:RequestTag` que requer que o cliente aplique as tags `costcenter=115` e `stack=prod` a todos os novos snapshots. Se os usuários não passarem essas tags específicas ou não especificarem nenhuma tag, haverá talha na solicitação.

Para ações de criação de recursos que aplicam tags, os clientes também devem ter permissões para usar a ação `CreateTags`. A terceira declaração usa a chave de condição `ec2:CreateAction` para permitir que os clientes criem tags somente no contexto de `CreateSnapshot`. Os clientes não podem marcar volumes existentes nem quaisquer outros recursos.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*"
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
```

```
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshot"
            }
         }
      }
   ]
}
```

Exemplo: criar snapshots de vários volume com etiquetas

A política a seguir inclui a chave de condição `aws:RequestTag`, que exige que o cliente aplique as etiquetas `costcenter=115` e `stack=prod` ao criar um conjunto de snapshots de vários volumes. Se os usuários não passarem essas tags específicas ou não especificarem nenhuma tag, haverá talha na solicitação.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*",
"arn:aws:ec2:*:*:volume/*"

   ]
      },
```

```
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshots"
            }
         }
      }
   ]
}
```

A política a seguir permite que os clientes criem um snapshot sem precisar especificar tags. A ação `CreateTags` só será avaliada se as tags forem especificadas na solicitação `CreateSnapshot` ou `CreateSnapshots`. Etiquetas podem ser omitidas na solicitação. Se uma tag for especificada, ela deverá ser `purpose=test`. Nenhuma outra tag é permitida na solicitação.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
```

```
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshot"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

A política a seguir permite que os clientes criem conjuntos de snapshots de vários volumes sem precisar especificar etiquetas. A ação `CreateTags` só será avaliada se as tags forem especificadas na solicitação `CreateSnapshot` ou `CreateSnapshots`. Etiquetas podem ser omitidas na solicitação. Se uma tag for especificada, ela deverá ser `purpose=test`. Nenhuma outra tag é permitida na solicitação.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshots"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

As seguintes políticas só permitirão que snapshots sejam criados se o volume de origem for marcado com `User:username` para o cliente, e o snapshot em si for marcado com `Environment:Dev` e `User:username`. O cliente pode adicionar outras tags ao snapshot.

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Environment":"Dev",
               "aws:RequestTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

A seguinte política de `CreateSnapshots` só permitirá que snapshots sejam criados se o volume de origem for marcado com `User:username` para o cliente e o snapshot em si for marcado com `Environment:Dev` e `User:username`.

```
{
   "Version":"2012-10-17",
```

```
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:instance/*",
 },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Environment":"Dev",
               "aws:RequestTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

A seguinte política só permitirá a exclusão de um snapshot se ele for marcado com o Usuário:usuário para o cliente.

```
{
   "Version":"2012-10-17",
   "Statement": [
            {
         "Effect":"Allow",
```

```
         "Action":"ec2:DeleteSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      }
   ]
}
```

A seguinte política permite que um cliente crie um snapshot mas negará a ação se o snapshot que está sendo criado tiver uma chave de tag `value=stack`.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

A seguinte política permite que um cliente crie snapshots, mas negará a ação se o snapshot que está sendo criado tiver uma chave de tag `value=stack`.

```
{
```

```
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

A política a seguir permite combinar várias ações em uma única política. Você só pode criar um snapshot (no contexto de `CreateSnapshots`) quando o snapshot é criado na região `us-east-1`. Você só pode criar snapshots (no contexto de `CreateSnapshots`) quando os snapshots são criados na região `us-east-1` e quando o tipo de instância é `t2*`.

```
{
   "Version":"2012-10-17",
   "Statement": [
          {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource": [
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ec2:*:*:snapshot/*",
            "arn:aws:ec2:*:*:volume/*"
         ],
```

```
        "Condition":{
           "StringEqualsIgnoreCase": {
             "ec2:Region": "us-east-1"
           },
           "StringLikeIfExists": {
             "ec2:InstanceType": ["t2.*"]
           }
        }
      }
   ]
}
```

Exemplo: Copiar snapshots

As permissões no nível do recurso especificadas para a ação CopySnapshot (Copiar snapshot) se aplicam somente ao novo snapshot. Elas não podem ser especificadas para o snapshot de origem.

A política de exemplo a seguir permite que as entidades copiem snapshots somente se o novo snapshot for criado com a chave de tag de `purpose` e um valor de tag de `production` (`purpose=production`).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCopySnapshotWithTags",
            "Effect": "Allow",
            "Action": "ec2:CopySnapshot",
            "Resource": "arn:aws:ec2:*:account-id:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "production"
                }
            }
        }
    ]
}
```

Exemplo: modificar configurações de permissão para snapshots

A política a seguir só permite a modificação de um snapshot se ele for marcado com `User:username`, em que `username` (nome de usuário) é o nome de usuário da conta da AWS do cliente. A solicitação falhará se essa condição não for atendida.

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:ModifySnapshotAttribute",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/user-name":"${aws:username}"
            }
         }
      }
   ]
}
```

Solução de problemas de identidade e acesso do Amazon EBS

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que você poderá enfrentar ao trabalhar com o Amazon EBS e o IAM.

Problemas

- Não tenho autorização para executar uma ação no Amazon EBS
- Não estou autorizado a executar iam:PassRole
- Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Amazon EBS

Não tenho autorização para executar uma ação no Amazon EBS

Se o AWS Management Console informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. Seu administrador é a pessoa que forneceu a você suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um volume, mas não tem as permissões de `ec2:DescribeVolumes`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeVolumes on resource: volume-id
```

Nesse caso, Mateo pede ao administrador da AWS para conceder a ele acesso ao volume.

Não estou autorizado a executar iam:PassRole

Caso receba uma mensagem de erro informando que você não tem autorização para executar a ação `iam:PassRole`, as políticas deverão ser atualizadas para permitir a transmissão de um perfil ao Amazon EBS.

Alguns Serviços da AWS permitem que você passe um perfil existente para o serviço, em vez de criar um novo perfil de serviço ou perfil vinculado ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro exemplificado a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para executar uma ação no Amazon EBS. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar a função para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se você precisar de ajuda, entre em contato com seu administrador da AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Amazon EBS

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon EBS é compatível com esses recursos, consulte Como o Amazon Elastic Block Store funciona com o IAM.
- Para saber como conceder acesso a seus atributos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Validação de conformidade para o Amazon Elastic Block Store

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte Referência dos Serviços Qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços com suporte e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no Amazon Elastic Block Store

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, throughputs elevadas e em redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que

automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura global da AWS.

Além da infraestrutura global da AWS, o Amazon EBS oferece vários recursos para ajudar a atender às suas necessidades de resiliência e backup de dados.

- Automatizar snapshots do EBS usando o Amazon Data Lifecycle Manager
- Copiar snapshots do EBS entre regiões

Monitorar o Amazon Elastic Block Store

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon Elastic Block Store e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar o Amazon EBS, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por você ou em seu nome Conta da AWS e entrega os arquivos de log em um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para mais informações, consulte o Guia do usuário do AWS CloudTrail.
- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- A Amazon EventBridge pode ser usada para automatizar seus AWS serviços e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

Tópicos

AWS CloudTrail para Amazon EBS

O Amazon Elastic Block Store (Amazon EBS) é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, por uma função ou por um serviço da AWS no Amazon EBS. O CloudTrail captura todas as chamadas de API para o Amazon EBS como eventos. As chamadas capturadas incluem chamadas do console do Amazon EBS e chamadas de código para as operações da API do Amazon EBS. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Amazon EBS. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Histórico de eventos. Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita ao Amazon EBS, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações sobre o Amazon EBS no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando uma atividade ocorre no Amazon EBS, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviço da AWS no Histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro de eventos em andamento na sua Conta da AWS, incluindo eventos do Amazon EBS, 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 eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especificou Além disso, é possível configurar outros serviços da AWS para analisar mais ainda e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Como receber arquivos de log do CloudTrail de várias regiões e Como receber arquivos de log do CloudTrail de várias contas

Todas as ações da API do Amazon EBS são registradas em log pelo CloudTrail. Por exemplo, as chamadas para as ações CreateVolume, DeleteVolume e CreateSnapshot geram entradas nos arquivos de log do CloudTrail.

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 usuário do IAM AWS Identity and Access Management
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento de identidade do usuário do CloudTrail.

Noções básicas sobre entradas de arquivos de log do Amazon EBS

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, 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, portanto não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação CreateVolume.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "Root",
        "principalId": "AROAJABCHBVMHREXAMPLE:root",
        "arn": "123456789012",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
    },
    "eventTime": "2024-02-08T08:02:21Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateVolume",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.12.123.123",
```

```
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
    "requestParameters": {
        "size": "100",
        "zone": "us-east-1a",
        "volumeType": "gp3",
        "iops": "3000",
        "encrypted": true,
        "masterEncryptionKeyId": "arn:aws:kms:us-east-1:123456789012:key/12345678-
a202-4b72-8030-example23456",
        "throughput": "125",
        "clientToken": "12345678-2427-4336-a555-e8607example"
    },
    "responseElements": {
        "requestId": "12345678-4229-4cfd-9cb1-0b094example",
        "volumeId": "vol-01234567890abcdef",
        "size": "100",
        "zone": "us-east-1a",
        "status": "creating",
        "createTime": 1707379341000,
        "volumeType": "gp3",
        "iops": 3000,
        "encrypted": true,
        "masterEncryptionKeyId": "arn:aws:kms:us-east-1:123456789012:key/12345678-
a202-4b72-8030-example23456",
        "tagSet": {},
        "multiAttachEnabled": false,
        "throughput": 125
    },
    "requestID": "12345678-4229-4cfd-9cb1-0b094example",
    "eventID": "12345678-4b33-4c18-90a1-76d4bexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

CloudWatch Métricas da Amazon para Amazon EBS

As CloudWatch métricas da Amazon são dados estatísticos que você pode usar para visualizar, analisar e definir alarmes sobre o comportamento operacional de seus volumes.

Os dados são disponibilizados automaticamente em períodos de um minuto, sem custo adicional.

Ao obter dados de CloudWatch, você pode incluir um parâmetro de `Period` solicitação para especificar a granularidade dos dados retornados. Esse período é diferente do que usamos quando coletamos os dados (períodos de um minuto). Recomendamos que você especifique em sua solicitação um período que seja igual ou maior do que o período de coleta para garantir que os dados retornados sejam válidos.

Você pode obter os dados usando a CloudWatch API ou o console do Amazon EC2. O console pega os dados brutos da CloudWatch API e exibe uma série de gráficos com base nos dados. Dependendo de suas necessidades, é possível preferir usar os dados da API ou os gráficos no console.

Tópicos

Métricas para volumes do Amazon EBS

O namespace `AWS/EBS` inclui as métricas a seguir para volumes do EBS que estão anexados a todos os tipos de instância. Todos os tipos de volume do Amazon EBS enviam automaticamente métricas de 1 minuto para CloudWatch, mas somente quando o volume é anexado a uma instância.

Para obter informações sobre o espaço em disco disponível do sistema operacional em uma instância, consulte Visualizar espaço livre em disco.

> **Note**
>
> Algumas métricas têm diferenças em instâncias criadas no sistema Nitro. Para obter uma lista desses tipos de instância, consulte Instâncias criadas no sistema Nitro.

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`VolumeReadBytes`	Fornece informações sobre as operações de leitura em um período especificado. • A estatística `Sum` reporta o número total de bytes transferidos durante o período. • A estatística `Average` informa o tamanho médio de cada operação de leitura durante o período, exceto em volumes anexados a uma instância do Nitro, em que a média se refere a um período especificado. • A estatística `SampleCount` informa o número total de operações de leitura durante o período, exceto nos volumes anexados a uma instância baseada em Nitro, em que a contagem de amostras representa o número de pontos de dados	Bytes	`VolumeId`	• `Average` • `Sum` • `SampleCount` • `Minimum` | `Maximum`: somente para volumes anexados a instâncias baseadas em Nitro

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
	utilizados no cálculo estatístico. **Note** Para instâncias de Xen, os dados são informados apenas quando há atividades de leitura no volume.			

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`VolumeWriteBytes`	Fornece informações sobre as operações de gravação em um período especificado. • A estatística `Sum` reporta o número total de bytes transferidos durante o período. • A estatística `Average` informa o tamanho médio de cada operação de gravação durante o período, exceto em volumes anexados a uma instância baseada em Nitro, em que a média se refere a um período especificado. • A estatística `SampleCount` informa o número total de operações de gravação durante o período, exceto nos volumes anexados a uma instância baseada em Nitro, em que a contagem de amostras representa o número de pontos de dados	Bytes	`VolumeId`	• `Average` • `Sum` • `SampleCount` • `Minimum` | `Maximum`: somente para volumes anexados a instâncias baseadas em Nitro

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
	utilizados no cálculo estatístico. **Note** Para instâncias de Xen, os dados são informados apenas quando há atividades de gravação no volume.			
`VolumeReadOps`	O número total de operações de leitura em um período especificado. As operações de leitura são contabilizadas na conclusão. Para calcular a média de operações de leitura por segundo (IOPS de leitura) para o período, divida o total das operações de leitura pelo número de segundos no período em questão.	Contagem	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum`: somente para volumes anexados a instâncias baseadas em Nitro

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`VolumeWriteOps`	O número total de operações de gravação em um período especificado. As operações de gravação são contadas na conclusão. Para calcular a média de operações de gravação por segundo (IOPS de gravação) para o período, divida o total das operações de gravação pelo número de segundos no período em questão.	Contagem	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum`: somente para volumes anexados a instâncias baseadas em Nitro

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`VolumeTotalReadTime`	**Note** Não é compatível com volumes habilitados Multi-Attach. Para instâncias de Xen, os dados são informados apenas quando há atividades de leitura no volume. O número total de segundos gastos por todas as operações de leitura que foram concluídas em um período especificado. Se várias solicitações são enviadas ao mesmo tempo, esse total pode ser maior do que a duração do período. Por exemplo, para um período de 1 minuto (60 segundos): se 150 operações foram concluídas durante esse período, e cada operação	Segundos	`VolumeId`	• `Average`: não é relevante para volumes anexados a instâncias baseadas em Nitro • `Sum` • `Minimum` | `Maximum`: somente para volumes anexados a instâncias baseadas em Nitro

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
	levou 1 segundo, o valor seria 150 segundos.			

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`VolumeTotalWriteTime`	**Note** Não é compatível com volumes habilitados Multi-Attach. Para instâncias de Xen, os dados são informados apenas quando há atividades de gravação no volume. O número total de segundos gastos por todas as operações de gravação que foram concluídas em um período especificado. Se várias solicitações são enviadas ao mesmo tempo, esse total pode ser maior do que a duração do período. Por exemplo, para um período de 1 minuto (60 segundos): se 150 operações foram concluídas durante esse período, e cada operação	Segundos	`VolumeId`	• `Average`: não é relevante para volumes anexados a instâncias baseadas em Nitro • `Sum` • `Minimum` | `Maximum`: somente para volumes anexados a instâncias baseadas em Nitro

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
	levou 1 segundo, o valor seria 150 segundos.			
`VolumeIdleTime`	**Note** Não é compatível com volumes habilitados Multi-Attach. O número total de segundos em um período de tempo especificado quando nenhuma operação de leitura ou de gravação foi enviada.	Segundos	`VolumeId`	• `Average`: não é relevante para volumes anexados a instâncias baseadas em Nitro • `Sum` • `Minimum` | `Maximum`: somente para volumes anexados a instâncias baseadas em Nitro

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`VolumeQueueLength`	O número de solicitações de operação de leitura e gravação aguardando conclusão em um período de tempo especificado.	Contagem	`VolumeId`	• `Average` • `Sum`: não é relevante para volumes anexados a instâncias do Nitro • `Minimum` | `Maximum`: somente para volumes anexados a instâncias do Nitro

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`VolumeStalledIOCheck`	**Note** Somente para instâncias do Nitro. Não publicado para volumes anexados ao Amazon ECS e AWS Fargate tarefas. Informa se um volume foi aprovado ou reprovado em uma verificação de E/S paralisada no último minuto. Essa métrica pode ser `0` (aprovada) ou 1 (reprovada).Para obter mais informações, consulte Monitore as características de E/S usando CloudWatch.	Contagem	`VolumeId` | `InstanceId`	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`VolumeThroughputPercentage`	**Note** Somente volumes SSD de IOPS provisionadas Não é compatível com volumes habilitados Multi-Attach. A porcentagem de operações de E/S por segundo (IOPS) entregues do total de IOPS provisionadas para um volume do Amazon EBS. Os volumes SSD de IOPS provisionadas fornecem a performance provisionada em 99,9% do tempo. Durante uma gravação, se não há outras solicitações pendentes de I/O em um minuto, o valor da métrica será 100%. Além disso, a performance de E/S de um volume pode se degradar temporariamente devido a uma ação que você tenha	Percentual	`VolumeId`	• `Average` • `Minimum` | `Maximum`

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
	realizado (por exemplo, criar um snapshot de um volume durante o uso máximo, executar o volume em uma instância não otimizada para EBS ou acessar dados no volume pela primeira vez).			

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`VolumeConsumedReadWriteOps`	**Note** Somente volumes SSD de IOPS provisionadas A quantidade total de operações de leitura e gravação (normalizada para unidades de capacidade de 256 K) consumida em um período especificado. As operações de I/O menores que 256 K contam como 1 IOPS consumida. Operações de I/O maiores que 256 K são contadas em unidades de capacidade de 256 K. Por exemplo, uma I/O de 1.024 K seria computada como 4 IOPS consumidas.	Contagem	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum`

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`BurstBalance`	**Note** `gp2`,`st1`, e somente `sc1` volumes. Fornece informações sobre a porcentagem de créditos de E/S (para `gp2`) ou de créditos de throughput (para `st1` e `sc1`) restante no bucket de intermitência. Os dados são reportados CloudWatch somente quando o volume está ativo. Se o volume não está conectado, nenhum dado é relatado. Se a performance basal do volume exceder a performance de expansão máxima, os créditos nunca serão gastos. Se o volume estiver anexado a uma instância criada no Sistema Nitro, o equilíbrio de expansão não será relatado. Para outras instâncias, o equilíbrio	Percentual	`VolumeId`	• `Average` • `Sum`: não é relevante para volumes anexados a instâncias Nitro. • `Minimum` | `Maximum`

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
	de expansão relatado é de 100%. Para ter mais informações, consulte Performance do volume gp2.			

Métricas para instâncias do Nitro

O namespace `AWS/EC2` inclui métricas adicionais do Amazon EBS para os volumes anexados a instâncias baseadas no Nitro que não são instâncias bare metal.

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSRead0ps`	Operações de leitura concluídas de todos os volumes do Amazon EBS anexados à instância em um período especificado. Para calcular a média de operações de E/S de leitura por segundo (IOPS de leitura) para o período, divida o total das operações pelo número de segundos no período em questão. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para calcular o IOPS de leitura. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função matemática CloudWatch métrica `DIFF_TIME` para encontrar as operações por segundo. Por exemplo, se você tiver representado graficamente `EBSRead0ps` CloudWatch como `m1`, a fórmula matemática métrica `m1/(DIFF_TIME(m1))` retornará	Contagem	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
	a métrica em operações/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções matemáticas métricas, consulte Usar matemática métrica no Guia CloudWatch do usuário da Amazon.		
`EBSWriteOps`	Operações de gravação concluídas para todos os volumes do EBS anexados à instância em um período especificado. Para calcular a média de operações de E/S de gravação por segundo (IOPS de gravação) para o período, divida o total das operações pelo número de segundos no período em questão. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para calcular o IOPS de gravação. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função matemática CloudWatch métrica `DIFF_TIME` para encontrar as operações por segundo. Por exemplo, se você tiver representado graficamente `EBSWriteOps` CloudWatch como`m1`, a fórmula matemática métrica `m1/(DIFF_TIME(m1))` retornará a métrica em operações/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções matemáticas métricas, consulte Usar matemática métrica no Guia CloudWatch do usuário da Amazon.	Contagem	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSReadBytes`	Bytes lidos de todos os volumes do EBS anexados à instância em um período especificado. O número relatado é o número de bytes lidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes lidos/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função matemática CloudWatch métrica `DIFF_TIME` para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `EBSReadBytes` CloudWatch como`m1`, a fórmula matemática métrica `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções matemáticas métricas, consulte Usar matemática métrica no Guia CloudWatch do usuário da Amazon.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSWriteBytes`	Bytes gravados em todos os volumes do EBS anexados à instância em um período especificado. O número relatado é o número de bytes gravados durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes gravados/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função matemática CloudWatch métrica `DIFF_TIME` para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `EBSWriteBytes` CloudWatch como `m1`, a fórmula matemática métrica `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções matemáticas métricas, consulte Usar matemática métrica no Guia CloudWatch do usuário da Amazon.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSIOBalance%`	Fornece informações sobre a porcentagem de créditos de E/S restantes no bucket de expansão. Essa métrica está disponível somente para monitoramento básico. Essa métrica está disponível apenas para alguns tamanhos de instância `*.4xlarge` e tamanhos menores que se expandam à performance máxima por apenas 30 minutos pelo menos uma vez a cada 24 horas. Para obter mais informações, consulte EBS otimizado por padrão. A estatística `Sum` não é aplicável a essa métrica.	Percentual	• Mínimo • Máximo
`EBSByteBalance%`	Fornece informações sobre a porcentagem de créditos de throughput restantes no bucket de expansão. Essa métrica está disponível somente para monitoramento básico. Essa métrica está disponível apenas para alguns tamanhos de instância `*.4xlarge` e tamanhos menores que se expandam à performance máxima por apenas 30 minutos pelo menos uma vez a cada 24 horas. Para obter mais informações, consulte EBS otimizado por padrão. A estatística `Sum` não é aplicável a essa métrica.	Percentual	• Mínimo • Máximo

Métricas para a restauração rápida do snapshot

O namespace `AWS/EBS` inclui as métricas a seguir para restauração rápida de snapshots.

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
`FastSnapshotRestoreCreditsBucketSize`	O número máximo do volume cria créditos que podem ser acumulados. Essa métrica é informada por snapshot e por zona de disponibilidade.	Contagem	`SnapshotId` | `AvailabilityZone`	• `Average` • `Minimum` | `Maximum` **Note** A estatística mais significativa é `Average`. Os resultados das estatísticas de `Minimum` e `Maximum` são iguais aos de `Average` e podem ser usados no lugar.
`FastSnapshotRestoreCreditsBalance`	O número do volume cria créditos disponíveis. Essa métrica é informada por snapshot e por zona de disponibilidade.	Contagem	`SnapshotId` | `AvailabilityZone`	• `Average` • `Minimum` | `Maximum` **Note** A estatística mais significativa é `Average`. Os resultados das estatísticas de `Minimum` e `Maximum`

Métrica	Descrição	Unidades	Dimensões	Estatísticas significativas
				são iguais aos de `Average` e podem ser usados no lugar.

Gráficos do console do Amazon EC2

Depois de criar um volume, você visualizará os gráficos de monitoramento de volumes no console do Amazon EC2. Selecione um volume na página Volumes no console e escolha Monitoring. A tabela a seguir lista os gráficos exibidos. A coluna à direita descreve como as métricas de dados brutos da CloudWatch API são usadas para produzir cada gráfico. O período de todos os gráficos é de cinco minutos.

Gráfico	Descrição usando métricas brutas
Throughput de leitura (KiB/s)	`Sum(VolumeReadBytes) / Period / 1024`
Throughput de gravação (KiB/s)	`Sum(VolumeWriteBytes) / Period / 1024`
Operações de leitura (Ops/s)	`Sum(VolumeReadOps) / Period`
Operações de gravação (Ops/s)	`Sum(VolumeWriteOps) / Period`
Comprimento médio de fila (operações)	`Avg(VolumeQueueLength)`
Tempo ocioso gasto (%)	`Sum(VolumeIdleTime) / Period × 100`

Tamanho médio de leitura (KiB/op)	`Avg(VolumeReadBytes) / 1024`
	
	Para instâncias baseadas em Nitro, a fórmula a seguir deriva o tamanho médio de leitura usando CloudWatch Metric Math:
	
	`(Sum(VolumeReadBytes) / Sum(VolumeReadOps)) / 1024`

Gráfico	Descrição usando métricas brutas
	As `VolumeReadOps` métricas `VolumeReadBytes` e estão disponíveis no CloudWatch console do EBS.

Tamanho médio de gravação (KiB/op)	`Avg(VolumeWriteBytes) / 1024`
	
	Para instâncias baseadas em Nitro, a fórmula a seguir deriva o tamanho médio de gravação usando CloudWatch Metric Math:
	
	`(Sum(VolumeWriteBytes) / Sum(VolumeWriteOps)) / 1024`
	
	As `VolumeWriteOps` métricas `VolumeWriteBytes` e estão disponíveis no CloudWatch console do EBS.

Latência média de leitura (ms/op)	`Avg(VolumeTotalReadTime) × 1000`
	
	Para instâncias baseadas em Nitro, a fórmula a seguir deriva a latência média de leitura usando Metric Math: CloudWatch
	
	`(Sum(VolumeTotalReadTime) / Sum(VolumeReadOps)) × 1000`
	
	As `VolumeReadOps` métricas `VolumeTotalReadTime` e estão disponíveis no CloudWatch console do EBS.

Latência média de gravação (ms/op)	`Avg(VolumeTotalWriteTime) × 1000`
	
	Para instâncias baseadas em Nitro, a fórmula a seguir deriva a latência média de gravação usando Metric Math: CloudWatch
	
	`(Sum(VolumeTotalWriteTime) / Sum(VolumeWriteOps)) * 1000`
	
	As `VolumeWriteOps` métricas `VolumeTotalWriteTime` e estão disponíveis no CloudWatch console do EBS.

Para os gráficos de latência média e os gráficos de tamanho médio, a média é calculada em relação ao número total de operações (leitura ou gravação, a que for aplicável ao gráfico) concluídas durante o período.

Amazon EventBridge para Amazon EBS

O Amazon EBS envia eventos para a Amazon EventBridge para ações realizadas em volumes e snapshots. Com EventBridge, você pode estabelecer regras que acionam ações programáticas em resposta a esses eventos. Por exemplo, você pode criar uma regra que envia uma notificação para seu e-mail quando um snapshot é habilitado para restauração rápida de snapshot.

Os eventos em EventBridge são representados como objetos JSON. Os campos que são exclusivos do evento estão contidos na seção "detalhes" do objeto JSON. O campo "evento" contém o nome do evento. O campo "resultados" contém o status concluído da ação que acionou o evento. Para obter mais informações, consulte os padrões de EventBridge eventos da Amazon no Guia EventBridge do usuário da Amazon.

Para obter mais informações, consulte O que é a Amazon EventBridge? no Guia do EventBridge usuário da Amazon.

Eventos

- Eventos de volume do EBS
- Eventos de modificação de volume do EBS
- Eventos de snapshot do EBS
- Eventos de arquivo de snapshots do EBS
- Eventos de restauração rápida do snapshot do EBS
- Usando AWS Lambda para lidar com EventBridge eventos

Eventos de volume do EBS

O Amazon EBS envia eventos para EventBridge quando os seguintes eventos de volume ocorrerem.

Eventos

- Criar volume (createVolume)
- Excluir volume (deleteVolume)

- Anexar ou reanexar volumes (attachVolume, reattachVolume)
- Desanexar volume (DetachVolume)

Criar volume (createVolume)

O `createVolume` evento é enviado para sua AWS conta quando uma ação para criar um volume é concluída. Contudo, não é salvo, registrado ou arquivado. Esse evento pode ter um resultado de `available` ou `failed`. A criação falhará se um AWS KMS key inválido for fornecido, conforme mostrado nos exemplos abaixo.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS para um evento `createVolume` bem-sucedido.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "available",
      "cause": "",
      "event": "createVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `createVolume` com falha. A causa da falha foi uma Chave do KMS desabilitada.

```
{
  "version": "0",
```

```
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

A lista a seguir é um exemplo de um objeto JSON emitido por EBS depois de um evento `createVolume` com falha. A causa da falha foi a importação pendente de uma Chave do KMS.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending import.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

Excluir volume (deleteVolume)

O `deleteVolume` evento é enviado para sua AWS conta quando uma ação para excluir um volume é concluída. Contudo, não é salvo, registrado ou arquivado. Esse evento tem o resultado `deleted`. Se a exclusão não for concluída, o evento nunca será enviado.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS para um evento `deleteVolume` bem-sucedido.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "deleted",
      "cause": "",
      "event": "deleteVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

Anexar ou reanexar volumes (attachVolume, reattachVolume)

O evento `attachVolume` ou o `reattachVolume` será enviado à sua conta da AWS se ocorrer uma falha ao associar ou reassociar um volume a uma instância. Contudo, não é salvo, registrado ou arquivado. Se você usar uma Chave do KMS para criptografar um volume do EBS e a Chave do KMS se tornar inválida, o EBS emitirá um evento se a Chave do KMS for usada posteriormente para associar ou reassociar a uma instância, conforme mostrado nos exemplos abaixo.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `attachVolume` com falha. A causa da falha foi a exclusão pendente de uma Chave do KMS.

> **Note**
>
> AWS pode tentar se reconectar a um volume após a manutenção de rotina do servidor.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "attachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `reattachVolume` com falha. A causa da falha foi a exclusão pendente de uma Chave do KMS.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
```

```
    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

Desanexar volume (DetachVolume)

O `detachVolume` evento é enviado para sua AWS conta quando um volume é separado de uma instância do Amazon EC2.

Dados de eventos

Veja a seguir um exemplo de um `detachVolume` evento bem-sucedido.

```
{
  "version":"0",
  "id":"2ec37298-1234-e436-70fc-c96b1example",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.ec2",
  "account":"123456789012",
  "time":"2024-03-18T16:35:52Z",
  "region":"us-east-1",
  "resources":[],
  "detail":
  {
    "eventVersion":"1.09",
    "userIdentity":
    {
      "type":"IAMUser",
      "principalId":"AIDAJT12345SQ2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/administrator",
      "accountId":"123456789012",
      "accessKeyId":"AKIAJ67890A6EXAMPLE",
      "userName":"administrator"
    },
    "eventTime":"2024-03-18T16:35:52Z",
    "eventSource":"ec2.amazonaws.com",
    "eventName":"DetachVolume",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"12.12.123.12",
```

```
    "userAgent":"aws-cli/2.7.12 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
ec2.detach-volume",
    "requestParameters":
    {
      "volumeId":"vol-072577c46bexample",
      "force":false
    },
    "responseElements":
    {
      "requestId":"1234513a-6292-49ea-83f8-85e95example",
      "volumeId":"vol-072577c46bexample",
      "instanceId":"i-0217f7eb3dexample",
      "device":"/dev/sdb",
      "status":"detaching",
      "attachTime":1710776815000
    },
    "requestID":"1234513a-6292-49ea-83f8-85e95example",
    "eventID":"1234551d-a15a-43eb-9e69-c983aexample",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "managementEvent":true,
    "recipientAccountId":"123456789012",
    "eventCategory":"Management",
    "tlsDetails":
    {
      "tlsVersion":"TLSv1.3",
      "cipherSuite":"TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader":"ec2.us-east-1.amazonaws.com"
    }
  }
}
```

Eventos de modificação de volume do EBS

O Amazon EBS envia `modifyVolume` eventos para EventBridge quando um volume é modificado. Contudo, não é salvo, registrado ou arquivado.

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

```
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
       "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
    ],
    "detail": {
       "result": "optimizing",
       "cause": "",
       "event": "modifyVolume",
       "request-id": "01234567-0123-0123-0123-0123456789ab"
    }
}
```

Eventos de snapshot do EBS

O Amazon EBS envia eventos para EventBridge quando os seguintes eventos de volume ocorrerem.

Eventos

- Criar snapshot (createSnapshot)
- Criar snapshots (createSnapshots)
- Copiar snapshot (copySnapshot)
- Compartilhar snapshot (shareSnapshot)

Criar snapshot (createSnapshot)

O `createSnapshot` evento é enviado para sua AWS conta quando uma ação para criar um instantâneo é concluída. Contudo, não é salvo, registrado ou arquivado. Esse evento pode ter um resultado de `succeeded` ou `failed`.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS para um evento `createSnapshot` bem-sucedido. Na seção `detail`, o campo `source` contém o ARN do volume de origem. Os campos `startTime` e `endTime` indicam quando a criação do snapshot começou e foi concluída.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
```

```
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
     "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "createSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-west-2:volume/vol-01234567",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"  }
}
```

Criar snapshots (createSnapshots)

O `createSnapshots` evento é enviado para sua AWS conta quando uma ação para criar um instantâneo de vários volumes é concluída. Esse evento pode ter um resultado de `succeeded` ou `failed`.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS para um evento `createSnapshots` bem-sucedido. Na seção `detail`, o campo `source` contém os ARNs dos volumes de origem do conjunto de snapshots de vários volumes. Os campos `startTime` e `endTime` indicam quando a criação do snapshot começou e foi concluída.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
```

```
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "completed"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "completed"
      }
    ]
  }
}
```

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `createSnapshots` com falha. A causa da falha foi a impossibilidade de conclusão de um ou mais snapshots do conjunto de snapshots de múltiplos volumes. Os valores de `snapshot_id` são os ARNs dos snapshots com falha. `startTime` e `endTime` representam quando a ação de criação de snapshots começou e terminou.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
"detail": {
    "event": "createSnapshots",
```

```
    "result": "failed",
    "cause": "Snapshot snap-01234567 is in status error",
   "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "error"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "error"
      }
    ]
  }
}
```

Copiar snapshot (copySnapshot)

O `copySnapshot` evento é enviado para sua AWS conta quando uma ação para copiar um instantâneo é concluída. Contudo, não é salvo, registrado ou arquivado. Esse evento pode ter um resultado de `succeeded` ou `failed`.

Se você estiver copiando o snapshot entre regiões, o evento será emitido na região de destino.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido pelo EBS após um evento `copySnapshot` bem-sucedido. O valor de `snapshot_id` é o ARN do snapshot recém-criado. Na seção `detail`, o valor de `source` é o ARN do snapshot de origem. `startTime` e `endTime` representam quando a ação copy-snapshot começou e terminou. `incremental` indica se o snapshot é um snapshot incremental (`true`) ou um snapshot completo (`false`).

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
```

```
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "incremental": "true"
  }
}
```

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `copySnapshot` com falha. A causa da falha era um ID de snapshot de origem inválido. O valor de `snapshot_id` é o nome de recurso da Amazon (ARN) do snapshot com falha. Na seção `detail`, o valor de `source` é o ARN do snapshot de origem. `startTime` e `endTime` representam o início e o fim da ação copy-snapshot.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
```

```
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Compartilhar snapshot (shareSnapshot)

O `shareSnapshot` evento é enviado para sua AWS conta quando outra conta compartilha um instantâneo com ela. Contudo, não é salvo, registrado ou arquivado. O resultado é sempre `succeeded`.

Dados de eventos

Veja a seguir um exemplo de um objeto JSON emitido pelo EBS depois de um evento `shareSnapshot` concluído. Na `detail` seção, o valor de `source` é o número da AWS conta do usuário que compartilhou o snapshot com você. `startTimee endTime` representam quando a ação de compartilhamento instantâneo começou e terminou. O evento `shareSnapshot` é emitido somente quando um snapshot privado é compartilhado com outro usuário. Compartilhar um snapshot público não aciona o evento.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "shareSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": 012345678901,
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Eventos de arquivo de snapshots do EBS

O Amazon EBS emite eventos relacionados a ações de arquivamento de snapshots. Para obter mais informações, consulte Monitorar o arquivamento de snapshots.

Eventos de restauração rápida do snapshot do EBS

O Amazon EBS envia eventos para EventBridge quando o estado de restauração rápida de um snapshot é alterado. Os eventos são emitidos com base no melhor esforço.

A seguir estão dados de exemplo para esse evento.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Fast Snapshot Restore State-change Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"
   ],
   "detail": {
      "snapshot-id": "snap-1234567890abcdef0",
      "state": "optimizing",
      "zone": "us-east-1a",
      "message": "Client.UserInitiated - Lifecycle state transition",
   }
}
```

Os valores possíveis para `state` são `enabling`, `optimizing`, `enabled`, `disabling` e `disabled`.

Os valores possíveis para `message` são os seguintes:

`Client.InvalidSnapshot.InvalidState - The requested snapshot transitioned to an invalid state (Error)`

A solicitação para habilitar a restauração rápida do snapshot falhou e o estado mudou para `disabling` ou `disabled`. A restauração rápida do snapshot não pode ser habilitada para esse snapshot.

`Client.UserInitiated`

O estado fez a transição para `enabling` ou `disabling`.

`Client.UserInitiated - Lifecycle state transition`

O estado fez a transição para `optimizing`, `enabled` ou `disabled`.

`Server.InsufficientCapacity - There was insufficient capacity available to satisfy the request`

A solicitação para habilitar a restauração rápida do snapshot falhou por capacidade insuficiente, e o estado mudou para `disabling` ou `disabled`. Espere e tente novamente.

`Server.InternalError - An internal error caused the operation to fail`

A solicitação para habilitar a restauração rápida do snapshot falhou por erro interno, e o estado mudou para `disabling` ou `disabled`. Espere e tente novamente.

`Client.InvalidSnapshot.InvalidState - The requested snapshot was deleted or access permissions were revoked`

Foi feita a transição do estado de restauração rápida de snapshots para `disabling` ou `disabled` porque o snapshot foi excluído ou não compartilhado pelo proprietário do snapshot. A restauração rápida de snapshots não pode ser habilitada para um snapshot que tenha sido excluído ou não seja mais compartilhado com você.

Usando AWS Lambda para lidar com EventBridge eventos

Você pode usar o Amazon EBS e a Amazon EventBridge para automatizar seu fluxo de trabalho de backup de dados. Isso exige que você crie uma política do IAM, uma AWS Lambda função para lidar com o evento e uma EventBridge regra que corresponda aos eventos recebidos e os encaminhe para a função Lambda.

O procedimento a seguir usa o evento `createSnapshot` para copiar automaticamente um snapshot concluído em outra região para recuperação de desastres.

Como copiar um snapshot concluído em outra região

1. Crie uma política do IAM, como a mostrada no exemplo a seguir, para fornecer permissões para usar a `CopySnapshot` ação e gravar no EventBridge registro. Atribua a política ao usuário que tratará do EventBridge evento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Defina uma função no Lambda que estará disponível no EventBridge console. O exemplo da função Lambda abaixo, escrito em Node.js, é invocado EventBridge quando um `createSnapshot` evento correspondente é emitido pelo Amazon EBS (significando que um snapshot foi concluído). Quando invocada, a função copia o snapshot de `us-east-2` em `us-east-1`.

```
// Sample Lambda function to copy an EBS snapshot to a different Region

var AWS = require('aws-sdk');
var ec2 = new AWS.EC2();

// define variables
var destinationRegion = 'us-east-1';
var sourceRegion = 'us-east-2';
console.log ('Loading function');

//main function
exports.handler = (event, context, callback) => {

    // Get the EBS snapshot ID from the event details
```

```
    var snapshotArn = event.detail.snapshot_id.split('/');
    const snapshotId = snapshotArn[1];
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;
    console.log ("snapshotId:", snapshotId);

    // Load EC2 class and update the configuration to use destination Region to
 initiate the snapshot.
    AWS.config.update({region: destinationRegion});
    var ec2 = new AWS.EC2();

    // Prepare variables for ec2.modifySnapshotAttribute call
    const copySnapshotParams = {
        Description: description,
        DestinationRegion: destinationRegion,
        SourceRegion: sourceRegion,
        SourceSnapshotId: snapshotId
    };

    // Execute the copy snapshot and log any errors
    ec2.copySnapshot(copySnapshotParams, (err, data) => {
        if (err) {
            const errorMessage = `Error copying snapshot ${snapshotId} to Region
 ${destinationRegion}.`;
            console.log(errorMessage);
            console.log(err);
            callback(errorMessage);
        } else {
            const successMessage = `Successfully started copy of snapshot
 ${snapshotId} to Region ${destinationRegion}.`;
            console.log(successMessage);
            console.log(data);
            callback(null, successMessage);
        }
    });
};
```

Para garantir que sua função Lambda esteja disponível no EventBridge console, crie-a na região em que o EventBridge evento ocorrerá. Para mais informações, consulte o Guia do desenvolvedor do AWS Lambda.

3. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
4. No painel de navegação, escolha Rules (Regras) e Create rule (Criar regras).
5. Em Step 1: Define rule detail (Etapa 1: definir detalhe da regra), faça o seguinte:

   a. Insira valores para Name (Nome) e Description (Descrição).
   b. Em Event bus (Barramento de eventos), mantenha o valor default (padrão).
   c. Certifique-se de que Enable the rule on the selected event bus (Habilitar a regra nos barramentos de eventos selecionados) esteja ativada.
   d. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).
   e. Escolha Próximo.
6. Em Step 2: Build event pattern (Etapa 2: criar padrão de evento), faça o seguinte:
   a. Em Origem do evento, selecione AWS eventos ou eventos de EventBridge parceiros.
   b. Na seção Padrão dos eventos, em Origem dos eventos, certifique-se de que a opção Serviço da AWS esteja selecionada e, em Serviço da AWS , selecione EC2.
   c. Em Event type (Tipo de evento), selecione EBS Snapshot Notification (Notificação de snapshot de EBS), selecione Specific event(s) (Eventos específicos) e, em seguida, selecione createSnapshot.
   d. Selecione Specific result(s) (Resultados específicos) e depois escolha succeeded (com êxito).
   e. Escolha Próximo.
7. Em Etapa 3: Select targets (Etapa 3: selecionar destinos), faça o seguinte:
   a. Em Tipos de destino, escolha Serviço da AWS .
   b. Em Select target (Selecionar destino), escolha Lambda function (Função do Lambda) e, em Function (Função), selecione a função criada anteriormente.
   c. Escolha Next (Avançar).
8. Em Step 4: Configure tags (Etapa 4: configurar etiquetas), especifique as etiquetas para a regra, se necessário e, em seguida, escolha Next (Avançar).
9. Em Step 5: Review and create (Etapa 5: revisar e criar), revise a regra e escolha Create rule (Criar regra).

A regra agora deve aparecer na guia Rules (Regras). No exemplo mostrado, o evento que você configurou deve ser emitido pelo EBS na próxima vez você copiar um snapshot.

Amazon GuardDuty para Amazon EBS

GuardDuty A Amazon é um serviço de detecção de ameaças que ajuda a proteger suas contas, contêineres, cargas de trabalho e os dados em seu AWS ambiente. Usando modelos de aprendizado de máquina (ML) e recursos de detecção de anomalias e ameaças, monitora GuardDuty continuamente diferentes fontes de log e atividades de tempo de execução para identificar e priorizar possíveis riscos de segurança e atividades maliciosas em seu ambiente.

O recurso de proteção contra malware incluído GuardDuty verifica os volumes do Amazon EBS associados às suas instâncias do Amazon EC2 e cargas de trabalho de contêineres para detectar possíveis ameaças. GuardDuty oferece duas maneiras de fazer isso:

- Habilite a proteção contra malware — Ao GuardDuty gerar uma descoberta indicativa da possível presença de malware em uma instância do Amazon EC2 ou em uma carga de trabalho de contêiner, ela iniciará automaticamente uma verificação de malware no recurso potencialmente comprometido.
- Use a verificação de malware sob demanda sem ativar a proteção contra malware — Forneça o nome de recurso da Amazon (ARN) da sua instância do Amazon EC2 para iniciar uma verificação sob demanda.

Para obter mais informações, consulte o Guia GuardDuty do usuário da Amazon.

Cotas do Amazon EBS

Sua Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada serviço da AWS service (Serviço da AWS). A menos que especificado de outra forma, cada cota é específica da região . Você pode solicitar o aumento de algumas cotas, porém, algumas delas não podem ser aumentadas.

Para visualizar todas as cotas do Amazon EBS, abra o console do Service Quotas. No painel de navegação, escolha Serviços da AWS e selecione Amazon Elastic Block Store (Amazon EBS). Para solicitar o aumento da cota, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas.

Sua Conta da AWS tem as cotas a seguir relacionadas ao Amazon EBS.

Nome	Padrão	Ajustá	Descrição
Snapshots arquivados por volume	Cada região com suporte: 25	Sim	O número máximo de snapshots arquivados por volume.
Solicitações de CompleteSnapshot por conta	Cada região compatível: 10 por segundo	Não	O número máximo de solicitações de CompleteSnapshot permitidas por conta.
Cópias simultâneas de snapshot por região de destino	Cada região compatível: 20	Não	O número máximo de cópias simultâneas de snapshot para uma única região de destino.
Snapshots simultâneos por volume de disco rígido frio (sc1)	Cada região compatível: 1	Não	O número máximo de snapshots simultâne os por volume de disco rígido frio (sc1) nesta região.
Snapshots simultâneos por volume SSD (gp2) de uso geral	Cada região compatível: 5	Não	O número máximo de snapshots simultâneos

Nome	Padrão	Ajustá	Descrição
			por volume SSD (gp2) de uso geral nesta região.
Snapshots simultâneos por volume de SSD (gp3) de uso geral	Cada região compatível: 5	Não	O número máximo de snapshots simultâneos por volume de SSD frio (gp3) nesta região.
Snapshots simultâneos por volume magnético (padrão)	Cada região compatível: 5	Não	O número máximo de snapshots simultâneos por volume magnético (padrão) nesta região.
Snapshots simultâneos por volume de SSD (io1) de IOPS provisionadas	Cada região compatível: 5	Não	O número máximo de snapshots simultâneos por volume SSD (io1) de IOPS provisionadas nesta região.
Snapshots simultâneos por volume SSD (io2) de IOPS provisionadas	Cada região compatível: 5	Não	O número máximo de snapshots simultâneos por volume SSD (io2) de IOPS provisionadas nesta região.
Snapshots simultâneos por volume de disco rígido (st1) otimizados para throughput	Cada região compatível: 1	Não	O número máximo de snapshots simultâne os por volume de disco rígido (sc1) otimizados para throughput nesta região.

Nome	Padrão	Ajustá	Descrição
Restauração rápida de snapshots	us-east-1: 5 us-east-2: 5 us-west-1: 5 us-west-2: 5 af-south-1: 5 ap-east-1: 5 ap-northeast-1: 5 ap-northeast-2: 5 ap-northeast-3: 5 ap-south-1: 5 ap-southeast-1: 5 ap-southeast-2: 5 ap-southeast-3: 5 ca-central-1: 5 eu-central-1: 5 eu-north-1: 5 eu-south-1: 5 eu-west-1: 5 eu-west-2: 5 eu-west-3: 5 me-south-1: 5	Sim	O número máximo de snapshots que podem ser habilitados para restauração rápida de snapshots nesta região.

Nome	Padrão	Ajustá	Descrição
	sa-east-1: 5 Cada uma das outras regiões compatíveis: 5		
Solicitações do GetSnapshotBlock por conta	Cada região compatível: 1.000 por segundo	Sim	O número máximo de solicitações GetSnapsh otBlock permitidas por conta.
Solicitações do GetSnapshotBlock por conta	Cada região compatível: 1.000 por segundo	Não	O número máximo de solicitações GetSnapsh otBlock permitidas por snapshot.
IOPS para volumes SSD de IOPS provisionadas (io1)	Cada região compatível: 300.000	Sim	O número máximo agregado de IOPS, que pode ser provisionado em volumes SDD de IOPS provisionados (io1) nesta região.
IOPS para volumes SSD de IOPS provisionados (io2)	Cada região compatível: 100.000	Sim	O número máximo agregado de IOPS, que pode ser provisionado em volumes SDD de IOPS provisionados (io2) nesta região.
Modificações de IOPS para volumes SSD de IOPS provisionados (io1)	Cada região compatível: 500.000	Sim	O número máximo agregado de IOPS, que pode ser solicitado provisionado em volumes SSD de IOPS provision ados (io1) nesta região.

Nome	Padrão	Ajustá	Descrição
Modificações de IOPS para volumes SSD de IOPS provisionados (io2)	Cada região compatível: 100.000	Sim	O máximo de IOPS atual (de) e solicitado (para) para solicitações de modificação de volume em volumes SSD de IOPS provisionadas (io2) nesta região.
Arquivos de snapshots simultâneos em andamento por conta	Cada região com suporte: 25	Sim	O número máximo de arquivos de snapshots em andamento por conta.
Restaurações de arquivos de snapshots simultâneos em andamento por conta	Cada região compatível: 5	Sim	O número máximo de restaurações de arquivos de snapshots em andamento por conta.
Solicitações do ListChangedBlocks por conta	Cada região compatível: 50 por segundo	Não	O número máximo de solicitações da API ListChangedBlocks permitidas por conta.
Solicitações do ListSnapshotBlocks por conta	Cada região compatível: 50 por segundo	Não	O número máximo de solicitações da API ListSnapshotBlocks permitidas por conta.
Snapshots pendentes por conta	Cada região com suporte: 100	Não	O número máximo de snapshots em um estado pendente por conta.
Solicitações do PutSnapshotBlock por conta	Cada região compatível: 1.000 por segundo	Sim	O número máximo de solicitações PutSnapsh otBlock permitidas por account.

Nome	Padrão	Ajustá	Descrição
Solicitações do PutSnapshotBlock por snapshot	Cada região compatível: 1.000 por segundo	Não	O número máximo de solicitações PutSnapsh otBlock permitidas por snapshot.
Snapshots por região	Cada região compatível: 100.000	Sim	Número máximo de snapshots por região
Solicitações do StartSnapshot por conta	Cada região compatível: 10 por segundo	Não	O número máximo de solicitações de StartSnap shot permitidas por account.
Armazenamento de volume de disco rígido frio (sc1) em TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada uma das outras regiões compatíveis: 50	Sim	A quantidade máxima agregada de armazenam ento, em TiB, que pode ser provisionada em volumes de disco rígido frio (sc1) nesta região.
Armazenamento para volumes SSD de uso geral (gp2), em TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada uma das outras regiões compatíveis: 50	Sim	A quantidade máxima agregada de armazenam ento, em TiB, que pode ser provisionada em volumes SSD de uso geral (gp2) nesta região.

Nome	Padrão	Ajustá	Descrição
Armazenamento para volumes SSD de uso geral (gp3), em TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada uma das outras regiões compatíveis: 50	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser provisionada em volumes SSD de uso geral (gp3) nesta região.
Armazenamento para volumes magnéticos (padrão), em TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada uma das outras regiões compatíveis: 50	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser provisionada em volumes magnéticos (padrão) nesta região.
Armazenamento para volumes SSD de IOPS provisionados (io1), em TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada uma das outras regiões compatíveis: 50	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser provisionada em volumes SSD de IOPS provisionados (io1) nesta região.

Nome	Padrão	Ajustá	Descrição
Armazenamento para volumes SSD de IOPS provisionados (io2), em TiB	Cada região compatível: 20	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser provisionada em volumes SSD de IOPS provisionados (io2) nesta região.
Armazenamento de volumes de disco rígido (st1) otimizados para throughput	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada uma das outras regiões compatíveis: 50	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser provisionada em volumes de disco rígido (sc1) otimizados para throughput nesta região.
Modificações de armazenamento de volume de disco rígido frio (sc1) em TiB	Cada região com suporte: 500	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser solicitada em modificações de volumes de disco rígido frio (sc1) nesta região.
Modificações de armazenamento para volumes SSD (gp2) de uso geral, em TiB	Cada região com suporte: 500	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser solicitada em modificações de volumes de SSD (gp2) de uso geral nesta região.

Nome	Padrão	Ajustá	Descrição
Modificações de armazenamento para volumes SSD (gp3) de uso geral, em TiB	Cada região com suporte: 500	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser solicitada em modificações de volumes de SSD (gp3) de uso geral nesta região.
Modificações de armazenamento para volumes magnéticos (padrão), em TiB	Cada região com suporte: 500	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser solicitada em modificações de volumes magnéticos (padrão) nesta região.
Modificações de armazenamento para volumes SSD de IOPS provisionados (io1), em TiB	Cada região com suporte: 500	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser solicitada em modificações de volumes SSD (io1) de IOPS provisionadas nesta região.
Modificações de armazenamento para volumes SSD de IOPS provisionados (io2), em TiB	Cada região compatível: 20	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser solicitada em modificações de volumes SSD (io2) de IOPS provisionadas nesta região.

Nome	Padrão	Ajustá	Descrição
Modificações de armazenamento de volumes de disco rígido (st1) otimizados para throughput	Cada região com suporte: 500	Sim	A quantidade máxima agregada de armazenamento, em TiB, que pode ser solicitada em modificações de volumes de disco rígido frio (sc1) otimizados para throughput nesta região.

Considerações

- Suas cotas podem mudar ao longo do tempo. O Amazon EBS monitora constantemente seu armazenamento provisionado e o uso de IOPS em cada região e pode aumentar automaticamente suas cotas, por região, com base no seu uso. Mesmo que o Amazon EBS possa aumentar automaticamente suas cotas com base no uso, é possível solicitar um aumento de cota, se necessário. Por exemplo, se você pretender usar mais armazenamento `gp3` no Leste dos EUA (Norte da Virgínia) do que o permitido por sua cota atual, poderá solicitar um aumento de cota para esse tipo de volume nessa região antes de iniciar o uso planejado.
- A cota para Cópias simultâneas de snapshots por região de destino não é ajustável usando Cotas de Serviço. No entanto, é possível solicitar um aumento para essa cota entrando em contato com o AWS Suporte.
- As cotas de modificações de IOPS e de armazenamento se aplicam ao valor atual agregado (por tamanho ou IOPS, dependendo da cota) de volumes que podem sofrer modificações simultaneamente. Você pode fazer solicitações de modificação simultâneas para volumes que combinaram o valor atual (por tamanho ou IOPS) até a cota. Por exemplo, se sua cota de modificações de IOPS para volumes SSD (io1) de IOPS provisionadas for `50,000`, você poderá fazer solicitações de modificações de IOPS simultâneas para qualquer número de `io1` volumes, desde que o IOPS atual combinado seja igual ou menor que `50,000`. Se você tiver três volumes `io1` provisionados com IOPS `20,000` cada, poderá solicitar modificações de IOPS para dois volumes simultaneamente (`20,000 * 2 < 50,000`). Se você enviar uma solicitação simultânea de modificação de IOPS para o terceiro volume, excederá sua cota e a solicitação falhará (`20,000 * 3 > 50,000`).

Histórico de documentos do Guia do usuário do Amazon EBS

A tabela a seguir descreve as versões da documentação do Amazon EBS.

Alteração	Descrição	Data
Habilite as políticas padrão do Amazon Data Lifecycle Manager em todas as contas	Você pode usar AWS CloudFormation StackSets para habilitar as políticas padrão do Amazon Data Lifecycle Manager em uma AWS organização ou em contas específicas. AWS	26 de abril de 2024
AWSDataLifecycleManagerSSMFullAccess AWS política gerenciada	Atualizada a política para garantir compatibilidade com snapshots consistentes com a aplicação para o SAP HANA usando o documento do SSM `AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA` .	17 de novembro de 2023
VolumeStalledMétricaIOCheck	Você pode usar a métrica `VolumeStalledIOCheck` para verificar se um volume foi aprovado ou reprovado em uma verificação de E/S paralisada no último minuto.	16 de novembro de 2023
Políticas padrão do Amazon Data Lifecycle Manager	Você agora pode criar políticas padrão do Amazon Data Lifecycle Manager para snapshots do EBS e AMIs baseadas no EBS para fazer	16 de novembro de 2023

	backup de todos os volumes e instâncias em uma região.	
Bloqueio de snapshots do Amazon EBS	Você pode bloquear os snapshots do Amazon EBS para protegê-los contra exclusões acidentais ou maliciosas, ou armazená-los no formato WORM por um período de tempo específico.	15 de novembro de 2023
Bloquear acesso público a snapshots	Agora você pode bloquear o acesso aos snapshots para evitar o compartilhamento público de seus snapshots.	9 de novembro de 2023
Scripts prévios e posteriores do Amazon Data Lifecycle Manager	Agora você pode usar scripts prévios e posteriores em suas políticas de snapshot do Amazon Data Lifecycle Manager para automatizar o ciclo de vida de snapshots consistentes com a aplicação.	7 de novembro de 2023
Reservas do NVMe	Os volumes `io2` habilitados para Multi-Attach oferecem suporte às reservas NVMe, que é um conjunto de protocolos de vedação de armazenamento padrão do setor.	18 de setembro de 2023

Testes de falhas no Amazon EBS	Use AWS FIS para interromper temporariamente a E/S entre um volume do EBS e as instâncias às quais ele está conectado para testar como suas cargas de trabalho lidam com interrupções de E/S.	27 de janeiro de 2023
Volumes `io2` do Block Express	Você pode modificar o tamanho e as IOPS provisionadas dos volumes do `io2` Block Express e pode habilitá-los para restauração rápida de snapshots.	31 de maio de 2022
Lixeira de snapshots do Amazon EBS	A lixeira de snapshots do Amazon EBS é um recurso de recuperação de snapshots que permite restaurar snapshots excluídos acidentalmente.	29 de novembro de 2021
Arquivo de snapshots do Amazon EBS	O arquivo de snapshots do Amazon EBS é uma nova camada de armazenamento que é possível usar para armazenamento de baixo custo e longo prazo dos snapshots acessados com pouca frequência.	29 de novembro de 2021
CloudWatch métricas para o Amazon Data Lifecycle Manager	Você pode monitorar suas políticas do Amazon Data Lifecycle Manager usando a Amazon. CloudWatch	28 de julho de 2021

CloudTrail eventos de dados para APIs diretas do EBS	As PutSnapshotBlock APIs ListSnapshotBlocks ListChangedBlocks GetSnapshotBlock,, e podem ser registradas em eventos de dados. CloudTrail	27 de julho de 2021
Volumes `io2` do Block Express	Os volumes `io2` do Block Express agora estão disponíveis para o público em geral.	19 de julho de 2021
Snapshots locais do Amazon EBS no Outposts	Agora é possível usar Snapshots locais do Amazon EBS em Outposts para armazenar snapshots de volumes em um Outpost localmente no Amazon S3 no próprio Outpost.	4 de fevereiro de 2021
Suporte Multi-Attach a volumes io2	Agora é possível habilitar volumes SSD de IOPS provisionadas (`io2`) para o Amazon EBS Multi-Attach.	18 de dezembro de 2020
Amazon Data Lifecycle Manager	Use o Amazon Data Lifecycle Manager para automatizar o processo de compartilhar snapshots e copiá-los entre contas. AWS	17 de dezembro de 2020
volumes gp3	Um novo tipo de volume de Finalidade geral (SSD) do Amazon EBS. É possível especificar IOPS provisionadas e throughput ao criar ou modificar o volume.	1º de dezembro de 2020

Tamanhos de volume de disco rígido otimizado e disco rígido frio com throughput	Os volumes de disco rígido (`st1`) Optimized Throughput (Throughput otimizada) (`sc1`) e disco rígido frio podem variar em tamanho de 125 GiB a 16 TiB.	30 de novembro de 2020
Amazon Data Lifecycle Manager	É possível usar o Amazon Data Lifecycle Manager para automatizar a criação, a retenção e a exclusão de AMIs suportadas pelo EBS.	9 de novembro de 2020
Amazon Data Lifecycle Manager	As políticas do Amazon Data Lifecycle Manager podem ser configuradas com até quatro programações.	17 de setembro de 2020
Volumes SSD (io2) com IOPS provisionadas para Amazon EBS	Volumes SSD de IOPS provisionadas (`io2`) são criados para fornecer 99,999% de durabilidade de volume com uma AFR até 0,001%.	24 de agosto de 2020
Restauração rápida de snapshots	É possível habilitar a restauraç ão rápida de snapshots compartilhados com você.	21 de julho de 2020
Amazon EBS Multi-Attach	Agora é possível anexar um único volume SSD de IOPS provisionadas (io1) a até 16 instâncias baseadas em Nitro que estejam na mesma zona de disponibilidade.	14 de fevereiro de 2020

Restaurações rápidas de snapshots do Amazon EBS	É possível habilitar restauraç ões rápidas de snapshots em um snapshot do EBS para garantir que os volumes do EBS criados a partir de um snapshot sejam totalment e inicializados na criação e entreguem instantaneamente toda a sua performance provisionada.	20 de novembro de 2019
Snapshots de vários volumes do Amazon EBS	Você pode obter instantân eos exatos point-in-time, coordenados com dados e consistentes em falhas em vários volumes do EBS conectados a uma instância do EC2.	29 de maio de 2019
Criptografia do Amazon EBS por padrão	Depois de habilitar a criptogra fia por padrão em uma região, todos os novos volumes do EBS que você criar nessa região serão criptografados usando a Chave do KMS padrão para criptografia do EBS.	23 de maio de 2019
Automatizar o ciclo de vida do snapshot	É possível usar o Amazon Data Lifecycle Manager para automatizar a criação e a exclusão de snapshots para seus volumes do EBS.	12 de julho de 2018

Executar modificações em volumes do EBS anexados	Com a maioria dos volumes do EBS anexados à maioria das instâncias do EC2, é possível modificar o tamanho, o tipo e as IOPS do volume sem desanexar o volume ou parar a instância.	13 de fevereiro de 2017
Copie snapshots criptografados do Amazon EBS entre Contas da AWS	Agora é possível copiar snapshots do EBS criptografados entre Contas da AWS.	21 de junho de 2016
Tipos de volumes HDD e HDD frio otimizados para throughput	Agora é possível criar HDD otimizado para throughput (st1) e volumes de disco rígido frio (sc1).	19 de abril de 2016
Tipo de volume SSD de uso geral	Os volumes Finalidade geral (SSD) oferecem armazenamento econômico ideal para uma ampla variedade de workloads. Esses volumes proporcionam latências de milissegundos de um dígito, capacidade de expansão de 3.000 IOPS por períodos estendidos e uma performance básica de 3 IOPS/GiB. Os volumes SSD de uso geral podem variar de tamanho entre 1 GiB e 1 TiB.	16 de junho de 2014

Criptografia do Amazon EBS	O Criptografia de Amazon EBS oferece criptografia sem interrupção dos volumes de dados do EBS, bem como de snapshots, eliminando a necessidade de criar e manter uma infraestrutura de gerenciamento de chaves de segurança. A criptografia do EBS ativa a segurança dos dados em repouso, criptogra fando os dados usando as Chaves gerenciadas pela AWS. A criptografia ocorre nos servidores que hospedam as instâncias do EC2, oferecendo criptografia de dados durante seu trânsito entre as instância s do EC2 e armazenamento do EBS.	21 de maio de 2014
Cópias incrementais de snapshots	Agora é possível executar cópias incrementais de snapshot.	11 de junho de 2013
Cópia de snapshots do EBS	É possível usar cópias de snapshots para criar backups de dados, para criar novos volumes do Amazon EBS ou para criar Imagens de máquina da Amazon (AMIs).	17 de dezembro de 2012

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.