Abordagens de backup e recuperação em AWS

# AWS Recomendações

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Recomendações: Abordagens de backup e recuperação em AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

# Table of Contents

Introdução ..... 1
Por que usar AWS como plataforma de proteção de dados? ..... 2
Resultados de negócios desejados ..... 4
Escolhendo AWS serviços ..... 5
Projetando uma solução de backup e recuperação ..... 7
AWS Backup ..... 8
Amazon S3 ..... 10
Uso de classes de armazenamento do Amazon S3 ..... 10
Criação de buckets do S3 padrão ..... 12
Usar o versionamento do Amazon S3 ..... 12
Fazendo backup e recuperando arquivos de configuração personalizados para AMIs ..... 12
Backup e restauração personalizados ..... 13
Proteger dados de backup ..... 13
Amazon EC2 com volumes do EBS ..... 15
Backup e recuperação do Amazon EC2 ..... 17
AMIs ou snapshots ..... 17
Volumes do servidor ..... 19
Volumes de servidor separados ..... 20
Volumes de armazenamento de instâncias ..... 20
Marcação e aplicação de padrões ..... 21
Criar backups de volume do EBS ..... 22
Preparação de um volume do EBS ..... 22
Criação de snapshots a partir do console ..... 24
Criação de AMIs ..... 24
Amazon Data Lifecycle Manager ..... 25
AWS Backup ..... 26
Multi-volume cópias de segurança ..... 26
Proteção de backups ..... 28
Como arquivar snapshots ..... 29
Automatização da criação de snapshots e AMI ..... 29
Restaurar um volume ou uma instância ..... 30
Restauração de arquivos e diretórios a partir de snapshots do EBS ..... 31
Restauração de um volume do EBS a partir de um snapshot do Amazon EBS ..... 31
Criação ou restauração de uma instância EC2 a partir de um snapshot do EBS ..... 33

Restauração de uma instância em execução a partir de uma AMI ..... 34
Backup e recuperação on-premises ..... 36
Gateway de arquivos ..... 37
Gateway de volumes ..... 37
Gateway de fitas ..... 38
Backup e recuperação de aplicativos ..... 40
Serviços AWS nativos em nuvem ..... 41
Amazon RDS ..... 41
Usar o DNS CNAME ..... 42
DynamoDB ..... 44
Arquiteturas híbridas ..... 46
Mover soluções centralizadas de gerenciamento de backup ..... 47
Recuperação de desastres ..... 49
On-premises DR para AWS ..... 49
DR para workloads nativos de nuvem ..... 51
DR em uma zona de disponibilidade única ..... 52
DR em uma falha regional ..... 52
Limpeza dos backups ..... 54
Perguntas frequentes ..... 55
Qual cronograma de backup devo selecionar? ..... 55
Preciso criar backups em minhas contas de desenvolvimento? ..... 55
Posso atualizar aplicativos e continuar usando um volume do EBS enquanto um snapshot estiver sendo criado sem qualquer impacto? ..... 55
Próximas etapas ..... 56
Recursos ..... 57
Histórico do documento ..... 58
..... lxi

# Abordagens de backup e recuperação em AWS

Khurram Nizami, Amazon Web Services (AWS)

Junho de 2024 (histórico do documento)

Este guia discute como implementar abordagens de backup e recuperação utilizando os serviços da Amazon Web Services (AWS) para arquiteturas on-premises, nativas de nuvem e híbridas. Essas abordagens oferecem custos mais baixos, maior escalabilidade e maior durabilidade para atender ao objetivo de tempo de recuperação (RTO), o objetivo de ponto de recuperação (RPO) e os requisitos de conformidade.

Este guia é destinado a líderes técnicos responsáveis pela proteção de dados em seus ambientes corporativos de TI e nuvem.

Este guia cobre diferentes arquiteturas de backup (aplicações nativas de nuvem, ambientes híbridos e on-premises). Também abrange os serviços associados da Amazon Web Services (AWS) que podem ser usados para criar soluções de proteção de dados escaláveis e confiáveis para os componentes não imutáveis de sua arquitetura.

Outra abordagem é modernizar suas cargas de trabalho para usar arquiteturas imutáveis, reduzindo a necessidade de backup e recuperação de componentes. AWS fornece vários serviços para implementar arquiteturas imutáveis e reduzir a necessidade de backup e recuperação, incluindo:

- Sem servidor com AWS Lambda
- Contêineres com Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) e AWS Fargate
- Amazon Machine Images (AMIs) com Amazon Elastic Compute Cloud (Amazon EC2)

À medida que o crescimento dos dados corporativos se acelera, a tarefa de protegê-los se torna mais desafiadora. Perguntas sobre a durabilidade e a escalabilidade das abordagens de backup são comuns, incluindo esta: Como a nuvem ajuda a atender às minhas necessidades de backup e restauração?

Este guia inclui os seguintes tópicos:

- Escolhendo AWS serviços para proteção de dados
- Projetando uma solução de backup e recuperação

- Backup e recuperação usando AWS Backup
- Backup e recuperação usando o Amazon S3
- Backup e recuperação para Amazon EC2 com volumes do EBS
- Backup e recuperação da infraestrutura local para AWS
- Backup e recuperação de aplicativos da AWS para o seu datacenter
- Backup e recuperação de serviços nativos em nuvem AWS
- Backup e recuperação para arquiteturas híbridas
- Recuperação de desastres com AWS
- Limpeza dos backups

## Por que usar AWS como plataforma de proteção de dados?

AWS é uma plataforma de computação em nuvem segura, de alto desempenho, flexível e easy-to-use econômica. AWS cuida do trabalho pesado indiferenciado necessário para criar, implementar e gerenciar soluções escaláveis de backup e recuperação.

Há muitas vantagens em usar AWS como parte de sua estratégia de proteção de dados:

- Durabilidade: o Amazon Simple Storage Service (Amazon S3) e o S3 Glacier Deep Archive foram projetados para oferecer 99,999999999% (11 noves) de durabilidade. Ambas as plataformas oferecem backup de dados confiável, com replicação de objetos em pelo menos três zonas de disponibilidade geograficamente dispersas. Muitos AWS serviços usam o Amazon S3 para armazenamento e export/import operações. Por exemplo, o Amazon Elastic Block Store (Amazon EBS) utiliza o Amazon S3 para armazenamento de snapshots.
- Segurança: AWS fornece várias opções para controle de acesso e criptografia de dados em trânsito e em repouso.
- Infraestrutura global: os AWS serviços estão disponíveis em todo o mundo, para que você possa fazer backup e armazenar dados na região que atendam aos seus requisitos de conformidade e carga de trabalho.
- Conformidade: a AWS infraestrutura é certificada quanto à conformidade com os seguintes padrões, para que você possa ajustar facilmente a solução de backup ao seu regime de conformidade existente:
  - Relatório Service Organization Controls (SOC)
  - Declaração sobre padrões para contratos de certificação (SSAE) 16

  - International Organization for Standardization (ISO) 27001
  - Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - SEC1
  - Federal Risk and Authorization Management Program (FedRAMP)
- Escalabilidade: com AWS, você não precisa se preocupar com a capacidade. Conforme suas necessidades mudarem, você poderá aumentar ou diminuir seu consumo sem sobrecarga administrativa.
- Menor custo total de propriedade (TCO): a escala das AWS operações reduz os custos do serviço e ajuda a reduzir o TCO dos AWS serviços. AWS repassa essa economia de custos aos clientes por meio de quedas de preços.
- Pay-as-you-go preços: adquira AWS serviços conforme necessário e somente pelo período em que planeja usá-los. AWS o preço não tem taxas iniciais, penalidades de rescisão ou contratos de longo prazo.

# Resultados de negócios desejados

O objetivo deste guia é fornecer uma visão geral dos AWS serviços que você pode usar para oferecer suporte às abordagens de backup e recuperação para o seguinte:

- Arquitetura on-premises
- Arquiteturas nativas de nuvem
- Arquiteturas híbridas
- AWS serviços nativos
- Recuperação de desastres (DR)

As melhores práticas e considerações são abordadas junto com uma visão geral dos serviços. Este guia também fornece as vantagens e desvantagens entre o uso de uma abordagem em detrimento de outra para backup e recuperação.

# Escolhendo AWS serviços para proteção de dados

AWS fornece vários serviços complementares e de armazenamento que podem ser usados como parte de sua abordagem de backup e recuperação. Esses serviços podem suportar arquiteturas híbridas e nativas de nuvem. Serviços diferentes são mais eficazes para casos de uso diferentes.

- O Amazon S3 é adequado para casos de uso híbridos e nativos da nuvem. Ele oferece soluções de armazenamento de objetos de uso geral altamente duráveis, adequadas para fazer backup de arquivos individuais, servidores ou um data center inteiro.
- AWS Storage Gateway é ideal para casos de uso híbridos. O Storage Gateway utiliza o poder do Amazon S3 para requisitos comuns de backup e armazenamento on-premises. Seus aplicativos se conectam ao serviço por meio de uma máquina virtual (VM) ou dispositivo de gateway de hardware usando os seguintes protocolos de armazenamento padrão:
  - Network File System (NFS)
  - Server Message Block (SMB)
  - Internet Small Computer System Interface (iSCSI)

  O gateway conecta esses protocolos locais comuns a serviços AWS de armazenamento, como os seguintes:
  - Amazon S3
  - S3 Glacier Deep Archive
  - Amazon EBS

  O Storage Gateway facilita o fornecimento de armazenamento elástico e de alto desempenho para arquivos, volumes, instantâneos e fitas virtuais. AWS
- AWS Backupé um serviço de backup totalmente gerenciado para centralizar e automatizar o backup de dados em todos os serviços. AWS Usando AWS Backup, você pode configurar centralmente as políticas de backup e monitorar a atividade de backup de recursos AWS , como os seguintes:
  - Volumes do EBS
  - Instâncias do EC2 (incluindo aplicativos Windows)
  - Bancos de dados do Amazon RDS e Amazon Aurora
  - Tabelas do DynamoDB
  - Bancos de dados do Amazon Neptune

- Bancos de dados Amazon DocumentDB (compatível com MongoDB)
- Sistemas de arquivos do Amazon EFS
- Sistemas de arquivos do Amazon FSx para Windows File Server e Amazon FSx para Lustre
- Volumes do Storage Gateway

O custo do AWS Backup é baseado no armazenamento que você consome, restaura e transfere em um mês. Para obter mais informações, consulte a Definição de preços do AWS Backup.

- Recuperação de desastres do AWS Elasticreplica suas máquinas em uma sub-rede de área de teste em sua região de destino Conta da AWS e preferida. O design da área de preparação reduz custos ao usar armazenamento acessível e recursos mínimos de computação para manter a replicação contínua. Você pode usar o Elastic Disaster Recovery para DR de on-premises para a nuvem e para DR entre regiões.
- AWS Configfornece uma visão detalhada da configuração dos AWS recursos em sua AWS conta. Isso inclui como os recursos estão relacionados entre si e como eles foram configurados. Nessa exibição, você pode ver como a configuração e os relacionamentos dos recursos mudaram ao longo do tempo.

  Ao ativar o registro de AWS Config configuração para seus AWS recursos, você mantém um histórico de seus relacionamentos de recursos ao longo do tempo. Isso ajuda a identificar e rastrear relacionamentos de AWS recursos (incluindo recursos excluídos) por até sete anos. Por exemplo, AWS Config pode rastrear a relação de um volume de snapshot do Amazon EBS e a instância EC2 à qual o volume foi anexado.
- AWS Lambda pode ser usado para definir e automatizar programaticamente seus procedimentos de backup e recuperação para seus workloads. Você pode usar os AWS SDKs para interagir com AWS os serviços e seus dados. Você também pode usar EventBridge a Amazon para executar suas funções do Lambda de forma programada.

AWS os serviços fornecem recursos específicos para backup e restauração. Para cada AWS serviço que você estiver usando, consulte a AWS documentação para determinar os recursos de backup, restauração e proteção de dados fornecidos pelo serviço. Você pode usar as operações AWS Command Line Interface (AWS CLI), AWS SDKs e API para automatizar os recursos AWS específicos do serviço para backup e recuperação de dados.

# Projetando uma solução de backup e recuperação

Ao desenvolver uma estratégia abrangente para fazer backup e restaurar dados, você deve primeiro identificar possíveis situações de falha ou desastre e seu potencial impacto nos negócios. Em alguns setores, você deve considerar os requisitos regulatórios de segurança de dados, privacidade e retenção de registros.

Os processos de backup e recuperação devem incluir o nível adequado de granularidade para atender ao objetivo de tempo de recuperação (RTO) e ao objetivo de ponto de recuperação (RPO) para o workload e seus processos de negócios de suporte, incluindo o seguinte:

- Recuperação em nível de arquivo (por exemplo, arquivos de configuração de um aplicativo)
- Recuperação em nível de dados do aplicativo (por exemplo, um banco de dados específico no MySQL)
- Recuperação no nível do aplicativo (por exemplo, uma versão específica do aplicativo do servidor web)
- Recuperação em nível de volume do Amazon EC2 (por exemplo, um volume do EBS)
- Recuperação em nível de instância do EC2. (por exemplo, uma instância EC2)
- Recuperação de serviços gerenciados (por exemplo, uma tabela do DynamoDB)

Certifique-se de considerar todos os requisitos de recuperação de sua solução e as dependências de dados entre vários componentes em sua arquitetura. Para facilitar um processo de restauração bem-sucedido, coordene o backup e a recuperação entre vários componentes em sua arquitetura.

Os tópicos a seguir descrevem abordagens de backup e recuperação com base na organização da sua infraestrutura. A infraestrutura de TI pode ser amplamente categorizada como on-premises, híbrida ou nativo de nuvem.

# Backup e recuperação usando AWS Backup

O AWS Backup é um serviço de backup totalmente gerenciado que centraliza e automatiza o backup de dados entre todos os serviços AWS. AWS Backup fornece uma camada de orquestração que integra o Amazon CloudWatch, AWS CloudTrail, AWS Identity and Access Management (IAM), AWS Organizations e outros serviços. Essa solução centralizada e nativa de nuvem AWS fornece recursos globais de backup que podem ajudá-lo a atingir seus requisitos de recuperação de desastres e conformidade. Usando o AWS Backup, você pode configurar centralmente as políticas de backup e monitorar a atividade de backup de recursos da AWS.

AWS Backup é a solução ideal para implementar planos de backup padrão para seus recursos AWS em suas contas AWS e Regiões. Como AWS Backup oferece suporte a vários tipos de recursos AWS, facilita a manutenção e a implementação de uma estratégia de backup para workloads usando vários recursos AWS que precisam ser copiados coletivamente. AWS Backup também permite monitorar coletivamente uma operação de backup e restauração que envolve vários recursos AWS.

Se você tiver requisitos de conformidade e auditoria, poderá utilizar o atributo AWS BackupAudit Manager para criar estruturas e relatórios de auditoria para apoiar seus requisitos de conformidade. O atributo AWS BackupVault Lock também oferece suporte aos requisitos de conformidade ao impor uma configuração WORM (Write Once, Read-Many) para todos os seus backups armazenados em um cofre de backup no AWS Backup.

Um diferencial importante do AWS Backup é o suporte para Organizations. Usando esse suporte, você pode definir e gerenciar políticas de backup no nível da organização ou da unidade organizacional e implementar automaticamente essas políticas para cada conta AWS e região relacionadas. Ao integrar novas contas AWS e regiões, você não precisa definir e gerenciar planos de backup separadamente.

AWS Backup pode facilitar a implementação de uma política de backup em toda a organização usando tags. Você pode criar planos de backup separados, cada um com configurações exclusivas de frequência e retenção e, em seguida, criar etiquetas exclusivas de pares de valores-chave que selecionam os recursos a serem incluídos no backup.

Por exemplo, você pode criar um plano de backup diário que inicie um backup às 05:00 UTC diariamente e tenha uma política de retenção de 35 dias. Esse plano de backup pode incluir uma atribuição de recurso de backup que especifique que qualquer recurso AWS suportado com o backup diário da chave de tag e o valor da tag será copiado de acordo com esse plano. Além disso, você pode criar um plano de backup mensal que comece às 05:00 UTC no primeiro dia de cada mês

e tenha uma política de retenção de 366 dias. Esse plano de backup pode incluir uma atribuição de recurso de backup que especifique que qualquer recurso da AWS suportado com o backup mensal da chave de tag e o valor da tag será copiado de acordo com esse plano.

Em seguida, você pode utilizar políticas de tags e a regra de tags obrigatórias AWS Config para garantir que todos os seus recursos AWS suportados tenham essa chave de tag e um desses valores de tag. Essa abordagem pode ajudá-lo a implementar e manter consistentemente uma abordagem de backup padrão em AWS para recursos AWS Backup suportados. Você pode estender essa abordagem para padronizar os backups de seus aplicativos e camadas arquitetônicas que tenham diferentes requisitos de objetivo de ponto de recuperação (RPO).

Recomendamos tomar medidas para proteger seu cofre de backup. Por exemplo, você pode implementar uma política de controle de serviços (SCP) da organização que impeça que seu cofre de backup seja excluído ou compartilhado com contas AWS indesejadas. Para obter mais detalhes e outras considerações importantes sobre segurança, consulte a postagem do blog As 10 melhores práticas de segurança para proteger backups em AWS.

AWS Backup pode simplificar a implementação de seu plano de recuperação de desastres (DR) para AWS porque ele oferece suporte a vários recursos AWS que podem ser tratados coletivamente. Por exemplo, você pode implementar backup entre regiões e entre contas para a maioria dos tipos de recursos AWS suportados por AWS Backup. O backup entre contas melhora a segurança do backup porque uma cópia está disponível em uma conta separada. O backup entre regiões melhora a disponibilidade porque os backups estão disponíveis em mais de uma região. Para obter detalhes sobre os tipos de recursos AWS compatíveis, consulte a tabela Disponibilidade de atributos por recurso.

Você pode utilizar o exemplo de Backup e Recuperação com solução de código aberto AWS Backup para implementar uma abordagem de infraestrutura como código (IaC) e integração contínua e entrega contínua (CI/CD) para gerenciar backups em sua organização AWS Organizations. Essa solução inclui atributos personalizados, como a reaplicação automática de tags AWS nos recursos AWS restaurados, bem como o estabelecimento de um cofre de backup secundário em uma conta e região separadas para fins de recuperação de desastres.

# Backup e recuperação usando o Amazon S3

Você pode usar o Amazon Simple Storage Service (Amazon S3) para armazenar e recuperar qualquer quantidade de dados, a qualquer momento. Você pode usar o Amazon S3 como seu armazenamento permanente para seus dados de aplicativos e processos de backup e restauração ao nível de arquivo. Por exemplo, você pode copiar seus backups de banco de dados de uma instância de banco de dados para o Amazon S3 com um script de backup usando o AWS CLI ou. AWS SDKs

Serviços da AWS use o Amazon S3 para armazenamento altamente durável e confiável, como nos exemplos a seguir:

- O Amazon EC2 usa o Amazon S3 para armazenar snapshots do Amazon EBS para volumes do EBS e para armazenamentos de instâncias do EC2.
- O Storage Gateway se integra ao Amazon S3 para fornecer ambientes on-premises com compartilhamentos de arquivos, volumes e bibliotecas de fitas compatíveis com o Amazon S3.
- O Amazon RDS usa o Amazon S3 para snapshots do banco de dados.

Muitas soluções de backup de terceiros também usam o Amazon S3. Por exemplo, o Arcserve Unified Data Protection é compatível com o Amazon S3 para backup durável de servidores on-premises e nativo de nuvem.

Você pode usar os atributos integrados ao Amazon S3 desses serviços para simplificar sua abordagem de backup e recuperação. Ao mesmo tempo, você pode se beneficiar da alta durabilidade e disponibilidade fornecidas pelo Amazon S3.

O Amazon S3 armazena dados como objetos dentro de recursos chamados de buckets. É possível armazenar quantos objetos desejar em um bucket. Você pode escrever, ler e excluir objetos em seu bucket com controle de acesso refinado. Objetos individuais devem ter tamanho de até 5 TB.

## Usar classes de armazenamento do Amazon S3 para reduzir os custos de armazenamento de dados de backup

O Amazon S3 oferece várias classes de armazenamento para uso em arquiteturas on-premises, híbridas e nativas da nuvem. Todas as classes de armazenamento oferecem capacidade escalável, que não é necessário gerenciamento de volume ou mídia à medida que seus conjuntos de dados de

backup crescem. O modelo pay-for-what-you de uso e o baixo custo por unidade GB/month tornam as classes de armazenamento do Amazon S3 adequadas para uma ampla variedade de casos de uso de proteção de dados. As classes de armazenamento do Amazon S3 foram projetadas para diferentes casos de uso, incluindo as seguintes categorias:

- Classes de armazenamento de acesso frequente para armazenamento de uso geral de dados acessados com frequência (por exemplo, arquivos de configuração, backups não planejados, backups diários). Isso inclui a classe de armazenamento S3 Standard, que é a padrão para todos os objetos Amazon S3.
- Classes de armazenamento de acesso pouco frequente para dados de longa duração, mas acessados com pouca frequência (por exemplo, backups mensais). Isso inclui a classe de armazenamento S3 Standard-IA. IA (Infrequent Access) é a sigla em inglês para acesso pouco frequente.
- Classes de armazenamento S3 Glacier para dados com vida útil extremamente longa que raramente precisam ser acessados (por exemplo, backups anuais). Isso inclui o S3 Glacier Deep Archive, que fornece o armazenamento de menor custo disponível. AWS

Para backups com padrões de acesso desconhecidos ou variáveis, você pode usar a classe de armazenamento S3 Intelligent-Tiering. O S3 Intelligent-Tiering transfere automaticamente os objetos para o nível mais econômico com base no número de dias desde o último acesso ao objeto.

> **Note**
>
> Algumas classes de armazenamento têm uma taxa de duração mínima. Para obter detalhes, consulte os preços do Amazon S3 e use a pesquisa da página da Web para encontrar `duration`.

O Amazon S3 também oferece políticas de ciclo de vida configuráveis para gerenciar seus dados durante o ciclo de vida. Depois que uma política for definida, seus dados serão migrados automaticamente para a classe de armazenamento apropriada, sem nenhuma alteração em sua aplicação. Para obter mais informações, consulte a documentação de Gerenciamento de ciclo de vida de objetos do Amazon S3.

Para reduzir seus custos de backup, use uma abordagem de classe de armazenamento em camadas com base no seu objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO), como no exemplo a seguir:

- Backups diários das últimas 2 semanas usando o S3 Standard
- Backups semanais dos últimos 3 meses usando o S3 Standard-IA
- Backups trimestrais do ano anterior no S3 Glacier Flexible Retrieval
- Backups anuais dos últimos 5 anos no S3 Glacier Deep Archive
- Backups excluídos do S3 Glacier Deep Archive após a marca de 5 anos

## Criação de buckets S3 padrão para backup e arquivamento

Você pode criar um bucket padrão do S3 para backup e arquivo, implementando a política de backup e retenção da sua empresa por meio de políticas de ciclo de vida do S3. A marcação de alocação de custos e os relatórios para AWS faturamento são baseados nas tags atribuídas no nível do bucket. Se a alocação de custos for importante, crie buckets S3 de backup e arquivamento separados para cada projeto ou unidade de negócios para que você possa alocar os custos adequadamente.

Seus scripts e aplicativos de backup podem usar o bucket S3 de backup e arquivamento que você cria para armazenar point-in-time instantâneos de dados de aplicativos e cargas de trabalho. Você pode criar um prefixo S3 padrão para ajudá-lo a organizar seus instantâneos de point-in-time dados. Por exemplo, se você criar backups de hora em hora, considere usar um prefixo de backup, como `YYYY/MM/DD/HH/<WorkloadName>/<files...>`. Ao fazer isso, você pode recuperar rapidamente seus point-in-time backups manual ou programaticamente.

## Usando o Versionamento do Amazon S3 para manter automaticamente o histórico de reversão

Você pode ativar o versionamento de objetos do S3 para manter um histórico das alterações do objeto, incluindo a capacidade de reverter para uma versão anterior. Isso é útil para arquivos de configuração e outros objetos que podem mudar com mais frequência do que sua agenda de point-in-time backup. Também é útil para arquivos que precisam ser revertidos individualmente.

## Usando o Amazon S3 para fazer backup e recuperar arquivos de configuração personalizados para AMIs

O Amazon S3 com controle de versionamento de objetos pode tornar-se seu sistema de registro para seus arquivos de opção e configuração da workload. Por exemplo, você pode usar uma imagem

padrão do AWS Marketplace Amazon EC2 que é mantida por um ISV. Essa imagem pode conter software cuja configuração é mantida em vários arquivos de configuração. Você pode manter seus arquivos de configuração personalizados no Amazon S3. Quando a sua instância é iniciada, você pode copiar esses arquivos de configuração para sua instância como parte dos dados de usuário da instância. Ao aplicar essa abordagem, você não precisa personalizar e recriar uma AMI para usar um versionamento atualizado.

## Usando o Amazon S3 em seu processo personalizado de backup e restauração

O Amazon S3 fornece um armazenamento de backup de uso geral que você pode integrar rapidamente aos seus processos existentes de backup personalizados. Você pode usar as operações de API AWS CLI AWS SDKs,, e para integrar seus scripts e processos de backup e restauração que usam o Amazon S3. Por exemplo, você pode ter um script de backup de banco de dados que realiza exportações do banco de dados durante a noite. Você pode personalizar esse script para copiar seus backups noturnos para o Amazon S3 para armazenamento externo. Consulte o tutorial sobre upload de arquivos em lote para a nuvem para ter uma visão geral de como fazer isso.

Você pode adotar uma abordagem semelhante para exportar e fazer backup de dados para diferentes aplicativos com base no seu RPO individual. Além disso, você pode usar AWS Systems Manager para executar seus scripts de backup em suas instâncias gerenciadas. O Systems Manager fornece automação, controle de acesso, agendamento, logging e notificação para seus processos individuais de backup.

## Proteção de dados de backup no Amazon S3

A segurança dos dados é uma preocupação universal e AWS leva a segurança muito a sério. A segurança é a base de cada AWS service (Serviço da AWS). O Amazon S3 oferece recursos de controle de acesso e criptografia tanto em repouso quanto em trânsito. Todos os endpoints do Amazon S3 são compatíveis com SSL/TLS para criptografar dados em trânsito. Você pode configurar a criptografia para objetos em repouso fazendo o seguinte:

- Usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (padrão)
- Usando criptografia do lado do servidor com chaves AWS Key Management Service (AWS KMS) armazenadas em AWS KMS

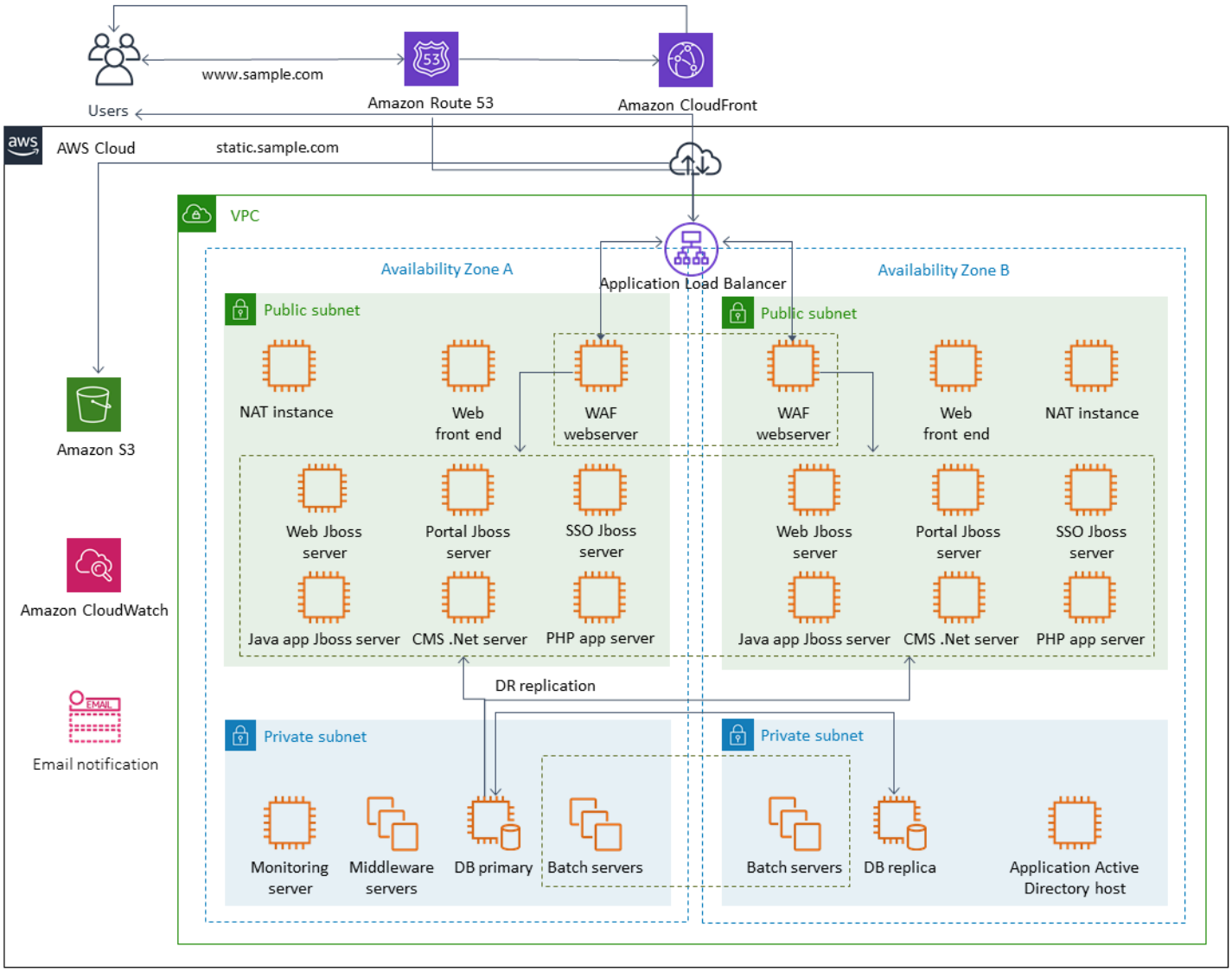
- Usando a criptografia do lado do cliente

Você pode usar AWS Identity and Access Management (IAM) para controlar o acesso aos objetos do S3. O IAM fornece controle sobre permissões para objetos individuais e caminhos de prefixos específicos em um bucket do S3. Você pode auditar o acesso aos objetos do S3 usando o registro em nível de objeto com. AWS CloudTrail

# Backup e recuperação para Amazon EC2 com volumes do EBS

AWS fornece vários métodos para fazer backup de suas instâncias do Amazon EC2. Esta seção aborda diferentes aspectos do backup de volumes do Amazon Elastic Block Store (Amazon EBS) ou volumes de armazenamento de instância para armazenamento. Considere AWS Backup sua primeira opção para gerenciar backups AWS se eles atenderem às suas necessidades. Lembre-se de que backups são úteis somente se puderem ser restaurados para a função para a qual foram destinados. A função de restauração e recuperação deve ser testada regularmente para confirmar isso.

A arquitetura da solução no diagrama a seguir descreve um ambiente de carga de trabalho que existe inteiramente AWS com a maioria da arquitetura baseada no Amazon EC2. Como mostra a figura a seguir, o cenário inclui servidores Web, servidores de aplicações, servidores de monitoramento, bancos de dados, Active Directory e replicação de recuperação de desastres (DR).




AWS fornece muitos serviços completos para muitos dos servidores Amazon EC2 representados nessa arquitetura para realizar o trabalho indiferenciado de criar, provisionar, fazer backup, restaurar e otimizar as instâncias e o armazenamento. Considere se esses serviços fazem sentido em sua arquitetura para reduzir a complexidade e o gerenciamento. AWS também fornece serviços para melhorar a disponibilidade de suas arquiteturas baseadas no Amazon EC2. Em particular, considere o Amazon EC2 Auto Scaling e o balanceador de carga elástico para complementar seus workloads no Amazon EC2. O uso desses serviços pode melhorar a disponibilidade e a tolerância a falhas da sua arquitetura e ajudá-lo a restaurar instâncias danificadas com o mínimo de impacto ao usuário.

As instâncias do EC2 utilizam principalmente volumes do Amazon EBS para armazenamento persistente. O Amazon EBS fornece vários atributos para backup e recuperação que são abordados em detalhes nesta seção.

Tópicos


- Backup e recuperação do Amazon EC2 com snapshots e AMIs
- Criação de backups de volume do EBS com AMIs e snapshots do EBS
- Restauração de um volume do Amazon EBS ou uma instância do EC2


# Backup e recuperação do Amazon EC2 com snapshots e AMIs

Considere se é necessário criar um backup completo de uma instância do EC2 com uma imagem de máquina da Amazon (AMI) ou tire um snapshot de um volume individual.

## Como utilizar AMIs ou snapshots do Amazon EBS para backups

Uma AMI inclui o seguinte:

- Um ou mais instantâneos. Instance-store-backed As AMIs incluem um modelo para o volume raiz da instância (por exemplo, um sistema operacional, um servidor de aplicativos e aplicativos).
- Permissões de lançamento que controlam quais AWS contas podem usar a AMI para iniciar instâncias.
- Um mapeamento de dispositivos de blocos que especifica os volumes a serem anexados à instância quando ela for executada.

> **Note**
>
> Na maioria dos casos, as AMIs para Windows, Red Hat, SUSE e SQL Server exigem que as informações corretas de licenciamento estejam presentes na AMI. Para obter mais informações, consulte Entender as informações de faturamento da AMI. Ao criar uma AMI de um snapshot, a operação `RegisterImage` obtém as informações de faturamento corretas dos metadados do snapshot, mas isso exige que os metadados apropriados estejam presentes. Para verificar se as informações de cobrança corretas foram aplicadas, verifique o campo Detalhes da plataforma na nova AMI. Se o campo estiver vazio ou não corresponder ao código do sistema operacional esperado (por exemplo, Windows, Red Hat, SUSE ou SQL), a criação da AMI não foi bem-sucedida e você deve descartar a AMI e seguir as instruções em Criar uma AMI a partir de uma instância.

Você pode utilizar AMIs para iniciar novas instâncias com software e dados pré-configurados. Você pode criar AMIs quando quiser estabelecer uma linha de base, que é uma configuração reutilizável para iniciar mais instâncias. Ao criar uma AMI de uma instância EC2 existente, um snapshot será criado para todos os volumes anexados à instância. O snapshot incluirá os mapeamentos do dispositivo.

Você não poderá utilizar snapshots para iniciar uma nova instância, mas pode utilizá-los para substituir volumes em uma instância existente. Caso você tenha dados corrompidos ou uma falha de volume, poderá criar um volume a partir de um snapshot que você tirou e substituir o volume antigo. Você também poderá utilizar snapshots para provisionar novos volumes e anexá-los durante a execução de uma nova instância.

Se você estiver usando AMIs de plataforma e aplicativo mantidas e publicadas pela AWS ou a partir da AWS Marketplace, considere manter volumes separados para seus dados. Você poderá fazer backup de seus volumes de dados como snapshots separados dos volumes do sistema operacional e do aplicativo. Em seguida, use os instantâneos do volume de dados com AMIs recém-atualizadas publicadas por AWS ou a partir do. AWS Marketplace Essa abordagem exige testes e planejamento cuidadosos para fazer backup e restaurar todos os dados personalizados, incluindo informações de configuração, nas AMIs recém-publicadas.

O processo de restauração é afetado pela sua escolha entre backups da AMI ou backups de snapshots. Se você criar AMIs para servir como backups de instância, deverá iniciar uma instância EC2 a partir da AMI como parte do processo de restauração. Talvez você também precise desligar a instância existente para evitar possíveis colisões. Um exemplo de uma possível colisão são os identificadores de segurança (SIDs) para instâncias do Windows associadas ao domínio. O processo de restauração de instantâneos pode exigir que você desconecte o volume existente e conecte o volume recém-restaurado. Ou talvez seja necessário fazer uma alteração na configuração para direcionar seus aplicativos para o volume recém-conectado.

AWS Backup suporta backups em nível de instância como AMIs e backups em nível de volume como instantâneos separados:

- Para um backup completo de todos os volumes do EBS na instância, crie uma AMI da instância do EC2. Quando quiser reverter, use o assistente de inicialização de instâncias para criar uma instância. No assistente de execução da instância, escolha Minhas AMIs.
- Para fazer backup de um volume individual, crie um snapshot. Para restaurar o snapshot, consulte Criar um volume a partir de um snapshot. Você pode usar o Console de gerenciamento da AWS ou o AWS Command Line Interface (AWS CLI).

O custo de uma AMI de instância é o armazenamento de todos os volumes na instância, mas não os metadados. O custo de um snapshot do EBS é o armazenamento do volume individual. Para obter mais informações sobre os custos de armazenamento em volume, consulte a página de preços do Amazon EBS..

## Volumes do servidor

Os volumes do EBS são a principal opção de armazenamento persistente para o Amazon EC2. Você pode utilizar esse armazenamento em bloco para dados estruturados, como bancos de dados, ou dados não estruturados, como arquivos em um sistema de arquivos em um volume.

Os volumes do EBS estão colocados em uma zona de disponibilidade específica. Os volumes são replicados em vários servidores para evitar perdas de dados causadas por falha em qualquer componente único. A falha se refere a uma perda total ou parcial do volume, dependendo do tamanho e do desempenho do volume.

Os volumes do EBS foram projetados para uma taxa anual de falhas (AFR) de 0,1 a 0,2%. Isso torna os volumes do EBS 20x mais confiável do que as unidades de disco típicas, que falham com um AFR de cerca de 4%. Por exemplo, se você tiver 1.000 volumes do EBS em execução por 1 ano, você deve esperar que um ou dois volumes falhem.

O Amazon EBS também oferece suporte a um atributo de snapshot para fazer backups pontuais de seus dados. Todos os tipos de volume EBS oferecem as mesmas capacidades de snapshots duráveis e foram projetados para disponibilidade de 99,999%. Para obter mais informações, consulte o Acordo de Nível de Serviço do Amazon Compute.

O Amazon EBS fornece a capacidade de criar snapshots (backups) de qualquer volume do EBS. Um snapshot é um atributo básico para criar backups de seus volumes do EBS. Um snapshot pega uma cópia do volume do EBS e o coloca no Amazon S3, onde ele é armazenado repetidamente em várias zonas de disponibilidade. O snapshot inicial é uma cópia completa do volume; os snapshots contínuos armazenam somente alterações incrementais em nível de bloco. Consulte a Documentação do Amazon EBS para obter detalhes sobre como criar snapshots do Amazon EBS.

Você pode realizar uma operação de restauração, excluir um snapshot ou atualizar os metadados do snapshot, como tags, associados ao snapshot do console do Amazon EC2 na mesma região em que você tirou o snapshot.

A restauração de um snapshot cria um novo volume do Amazon EBS com dados de volume completos. Se você precisar apenas de uma restauração parcial, poderá anexar o volume à instância

em execução com um nome de dispositivo diferente. Em seguida, monte-o e use os comandos de cópia do sistema operacional para copiar os dados do volume de backup para o volume de produção.

Os snapshots do Amazon EBS também podem ser copiados entre AWS regiões usando o recurso de cópia de instantâneos do Amazon EBS, conforme descrito na documentação do Amazon EBS. Você pode utilizar esse atributo para armazenar seu backup em outra região sem precisar gerenciar a tecnologia de replicação subjacente.

## Como estabelecer volumes de servidor separados

Você já pode utilizar um conjunto padrão de volumes separados para o sistema operacional, logs, aplicativos e dados. Ao estabelecer volumes de servidor separados, você poderá reduzir o escopo do impacto quando houver falhas no aplicativo ou na plataforma causadas pela exaustão do espaço em disco. Esse risco geralmente é maior com discos rígidos físicos, porque você não tem a flexibilidade de expandir volumes rapidamente. Com unidades físicas, você deverá comprar as novas unidades, fazer backup dos dados e depois restaurar os dados nas novas unidades. Com isso AWS, esse risco é bastante reduzido porque você pode usar o Amazon EBS para expandir seus volumes provisionados. Para obter mais informações, consulte a documentação do AWS.

Mantenha volumes separados para dados de aplicativos, dados do usuário, registros e arquivos de troca para que você possa utilizar políticas separadas de backup e restauração para esses recursos. Ao separar os volumes dos seus dados, você também poderá utilizar diferentes tipos de volume com base nos requisitos de desempenho e armazenamento dos dados. Em seguida, você poderá otimizar e ajustar seus custos para diferentes workloads.

## Considerações para volumes de armazenamento de instância

Um armazenamento de instâncias fornece armazenamento temporário em nível de bloco para a instância. Esse armazenamento está localizado em discos que estão anexados fisicamente ao computador host. Os armazenamentos de instância são ideais para armazenamento temporário de informações que mudam com frequência, como buffers, caches, dados temporários e outros conteúdos temporários. Eles também são preferíveis para dados replicados em toda a frota de instâncias, tal como um grupo com balanceador de carga de servidores web.

Os dados em um armazenamento de instâncias persistem apenas durante a vida útil da instância associada. Se uma instância for reiniciada (intencionalmente ou acidentalmente), dados no armazenamento de instância persistirão. Contudo, os dados no armazenamento de instâncias serão perdidos em qualquer das seguintes circunstâncias:

- A unidade de disco subjacente falha.
- A instância é interrompida.
- A instância é encerrada.

Portanto, não dependa do armazenamento de instâncias para dados valiosos de longo prazo. Em vez disso, use um armazenamento físico de dados mais durável, como Amazon S3, Amazon EBS ou Amazon EFS.

Uma estratégia comum com volumes de armazenamento de instância é manter os dados necessários no Amazon S3 regularmente, conforme necessário, com base no objetivo de ponto de recuperação (RPO) e no objetivo de tempo de recuperação (RTO). Em seguida, você poderá baixar os dados do Amazon S3 para o seu armazenamento de instância quando uma nova instância for iniciada. Você também poderá fazer o upload dos dados para o Amazon S3 antes que uma instância seja interrompida. Para persistência, crie um volume do EBS, anexe-o à sua instância e copie os dados do volume de armazenamento de instância para o volume do EBS periodicamente. Para obter mais informações, consulte o AWS Centro de Conhecimentos.

## Marcação e aplicação de padrões para snapshots e AMIs do EBS

Marcar todos os seus AWS recursos é uma prática importante para alocação de custos, auditoria, solução de problemas e notificação. A marcação é importante para volumes do EBS para que as informações pertinentes e necessárias para gerenciar e restaurar volumes estejam presentes. As tags não são copiadas automaticamente das instâncias do EC2 para as AMIs ou dos volumes de origem para os snapshots. Certifique-se de que seu processo de backup inclua as tags relevantes dessas fontes. Isso ajuda a definir os metadados do snapshot, como políticas de acesso, informações de anexo e alocação de custos, para usar esses back-ups futuramente. Para obter mais informações sobre como marcar seus AWS recursos, consulte o artigo técnico sobre melhores práticas de marcação.

Além das tags que você usa para todos os AWS recursos, use as seguintes tags específicas de backup:

- ID da instância de origem
- ID do volume de origem (para snapshots)
- Descrição do ponto de recuperação

Você pode aplicar políticas de marcação usando AWS Config regras e permissões do IAM. O IAM suporta o uso forçado de tags, para que você possa escrever políticas do IAM que exijam o uso de tags específicas ao atuar em snapshots do Amazon EBS. Se uma operação `CreateSnapshot` for tentada sem que as tags definidas na política de permissões do IAM concedam direitos, a criação do snapshot falhará com o acesso negado. Para obter mais informações, consulte a postagem do blog sobre marcação de snapshots do Amazon EBS na criação e implementação de políticas de segurança mais fortes.

Você pode usar AWS Config regras para avaliar automaticamente as configurações dos seus AWS recursos. Para ajudar você a começar, AWS Config fornece regras predefinidas e personalizáveis chamadas regras gerenciadas. Você também pode criar suas próprias regras. Enquanto monitora AWS Config continuamente as alterações de configuração entre seus recursos, ele verifica se essas alterações violam alguma das condições em suas regras. Se um recurso violar uma regra, AWS Config sinaliza o recurso e a regra como não compatíveis. Observe que a regra gerenciada por tags obrigatórias atualmente não oferece suporte a snapshots e AMIs.

# Criação de backups de volume do EBS com AMIs e snapshots do EBS

AWS fornece uma variedade de opções para criar e gerenciar AMIs e snapshots. Use a abordagem que satisfaça suas necessidades. Um problema comum que muitos clientes enfrentam é gerenciar o ciclo de vida dos snapshots e alinhá-los claramente por finalidade, política de retenção etc. Sem a marcação adequada, há o risco de que os snapshots sejam excluídos acidentalmente ou como parte de um processo de limpeza automatizado. Você também pode acabar pagando por snapshots obsoletos que são retidos porque não há um entendimento claro se eles ainda são necessários.

## Preparação de um volume do EBS antes de criar um snapshot ou AMI

Antes de tirar um snapshot ou criar uma AMI, faça os preparativos necessários para seu volume do EBS. A criação de uma AMI resulta em um novo snapshot para cada volume do EBS anexado à instância, portanto, essas preparações também se aplicam às AMIs.

É possível tirar um snapshot de um volume do EBS anexado que esteja em uso por uma instância EC2 desenvolvida. No entanto, os snapshots só capturam dados gravados no seu volume do EBS no momento em que o comando do snapshot é emitido. Isso pode excluir quaisquer dados em cache por aplicativos ou sistemas operacionais. A melhor prática é ter o sistema em um estado em que ele não esteja executando nenhum I/O. Idealmente, a máquina não está aceitando tráfego e está parada, mas isso é raro, pois as operações de 24/7 TI se tornam a norma. Se você puder extrair

qualquer dado da memória do sistema para o disco que está sendo usado pelos seus aplicativos e pausar a gravação de qualquer arquivo para o volume por tempo suficiente para tirar um snapshot, seu snapshot deverá estar completo.

Para fazer um backup limpo, você deverá desativar o banco de dados ou o sistema de arquivos. A forma como você faz isso dependerá do seu banco de dados ou do sistema de arquivos.

O processo para um banco de dados é o seguinte:

1. Se possível, coloque o banco de dados no modo de backup dinâmico.
2. Execute os comandos de snapshot do Amazon EBS.
3. Retire o banco de dados do modo de backup dinâmico ou, se estiver usando uma réplica de leitura, encerre a instância da réplica de leitura.

O processo de um sistema de arquivos é semelhante, mas depende dos recursos do sistema operacional ou do sistema de arquivos. Por exemplo, o XFS é um sistema de arquivos que pode liberar seus dados para um backup consistente. Para obter mais informações, consulte xfs_freeze. Como alternativa, você pode facilitar esse processo usando um gerenciador de volume lógico que ofereça suporte ao congelamento de I/O.

No entanto, se você não conseguir limpar ou pausar todas as gravações de arquivos no volume, faça o seguinte:

1. Desmonte o volume do sistema operacional.
2. Execute o comando de snapshot.
3. Remonte o volume para obter um snapshot consistente e completo. É possível remontar e usar o volume enquanto o status do snapshot está como pendente .

O processo de captura do snapshot continuará em segundo plano e a criação de snapshots será rápida e capturará um momento específico. Os volumes dos quais você está fazendo backup serão desmontados por apenas alguns segundos. Você poderá programar uma pequena janela de backup em que uma interrupção será esperada e tratada pelos clientes normalmente.

Para criar um snapshot para um volume do EBS que serve como dispositivo raiz, interrompa a instância antes de tirar o snapshot. O Windows fornece o Volume Shadow Copy Service (VSS) para ajudar a criar instantâneos consistentes com aplicativos. AWS fornece um documento do Systems Manager que você pode executar para fazer backups de aplicativos em nível de VSS-aware imagem. Os snapshots incluem dados das 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 a documentação do AWS.

> **Note**
>
> Se você estiver criando uma AMI do Windows para poder implantar outra instância semelhante, use EC2Config ou EC2Launch para fazer o Sysprep da sua instância. Em seguida, crie uma nova AMI a partir da instância interrompida. O Sysprep remove informações exclusivas da instância Windows do Amazon EC2, incluindo os SIDs, o nome do computador e os drivers. SIDs duplicados podem causar problemas com o Active Directory, o Windows Server Update Services (WSUS), problemas de login, ativação da chave de volume do Windows, Microsoft Office e produtos de terceiros. Não use o Sysprep com sua instância se sua AMI for para fins de backup e você quiser restaurar a mesma instância com todas as informações exclusivas intactas.

## Criação manual de snapshots de volume do EBS a partir do console

Crie snapshots dos volumes apropriados ou de toda a instância antes de fazer qualquer alteração importante que não tenha sido totalmente testada na instância. Por exemplo, talvez você queira criar um snapshot antes de atualizar ou corrigir o software do aplicativo ou do sistema na sua instância.

Você pode criar um snapshot manualmente a partir do console. No console do Amazon EC2, na página Volumes do Elastic Block Store, selecione o volume do qual você deseja fazer backup. Em seguida, no menu Actions, escolha Create snapshot. Você pode pesquisar volumes anexados a uma instância específica inserindo o ID da instância na caixa de filtro.

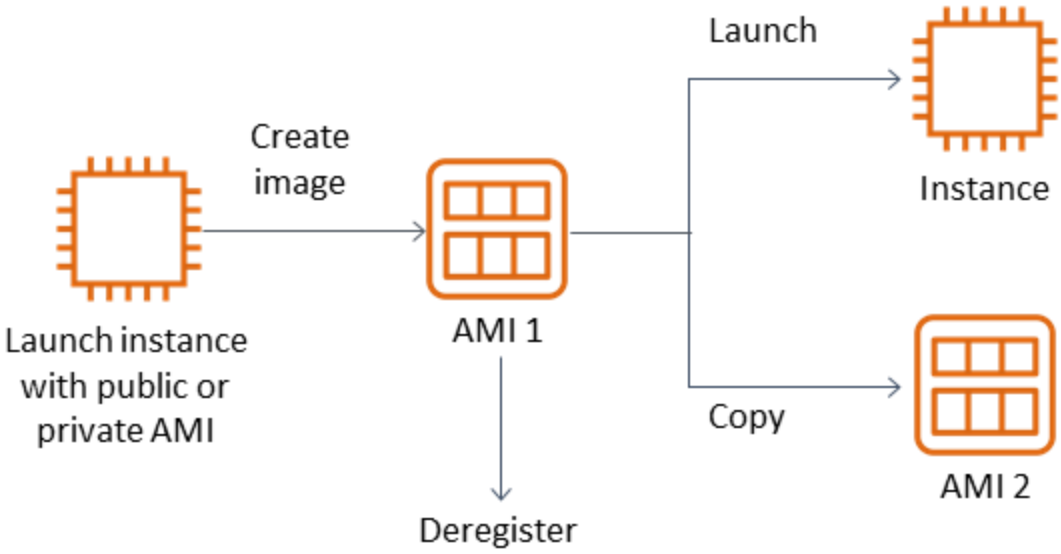
Insira uma descrição e adicione as tags apropriadas. Adicione uma tag `Name` para facilitar a localização do volume posteriormente. Adicione outras tags apropriadas com base na sua estratégia de marcação.

## Criação de AMIs

Uma AMI fornece as informações necessárias para iniciar uma instância. A AMI inclui o volume raiz e os snapshots dos volumes do EBS anexados à instância quando a imagem foi criada. Você não poderá iniciar novas instâncias apenas a partir de snapshots do EBS; você deverá iniciar novas instâncias a partir de uma AMI.

Quando você criar uma AMI, ela será criada na conta e na região que você estiver usando. O processo de criação da AMI cria snapshots do Amazon EBS para cada volume anexado à instância, e a AMI se refere a esses snapshots do Amazon EBS. Esses snapshots residem no Amazon S3 e são altamente duráveis.

Após criar uma AMI da sua instância EC2, você poderá utilizar a AMI para recriar a instância ou iniciar mais cópias da instância. Você também poderá copiar AMIs de uma região para outra para migração de aplicativos ou DR.




Uma AMI deve ser criada a partir de uma instância do EC2, a menos que você esteja migrando uma máquina virtual, como uma máquina virtual VMWARE, para o. AWS Para criar uma AMI a partir do console do Amazon EC2, selecione a instância, escolha Ações, escolha Imagem e, em seguida, escolha Criar imagem.

## Amazon Data Lifecycle Manager

É possível usar o Amazon Data Lifecycle Manager para automatizar a criação, a retenção e a exclusão de AMIs compatíveis com o EBS. A automação do gerenciamento de snapshots ajuda você a fazer o seguinte:

- Proteger dados valiosos impondo uma programação regular de backup.
- Reter os backups conforme exigido por auditores ou pelas regras de conformidade interna.
- Reduzir os custos de armazenamento ao excluir backup obsoletos.

Usando o Amazon Data Lifecycle Manager, você pode automatizar o processo de gerenciamento de snapshots para instâncias EC2 (e seus volumes EBS anexados) ou volumes EBS separados. Ele oferece suporte a opções como cópia entre regiões, para que você possa copiar snapshots automaticamente para outras regiões AWS . Copiar snapshots para regiões alternativas é uma abordagem para apoiar os esforços de DR e as opções de restauração em uma região alternativa. Você também pode utilizar o Amazon Data Lifecycle Manager para criar uma política de ciclo de vida de snapshots que ofereça suporte à restauração rápida de snapshots.

O Amazon Data Lifecycle Manager é um atributo incluído do Amazon EC2 e do Amazon EBS. Não há cobrança para o Amazon Data Lifecycle Manager.

## AWS Backup

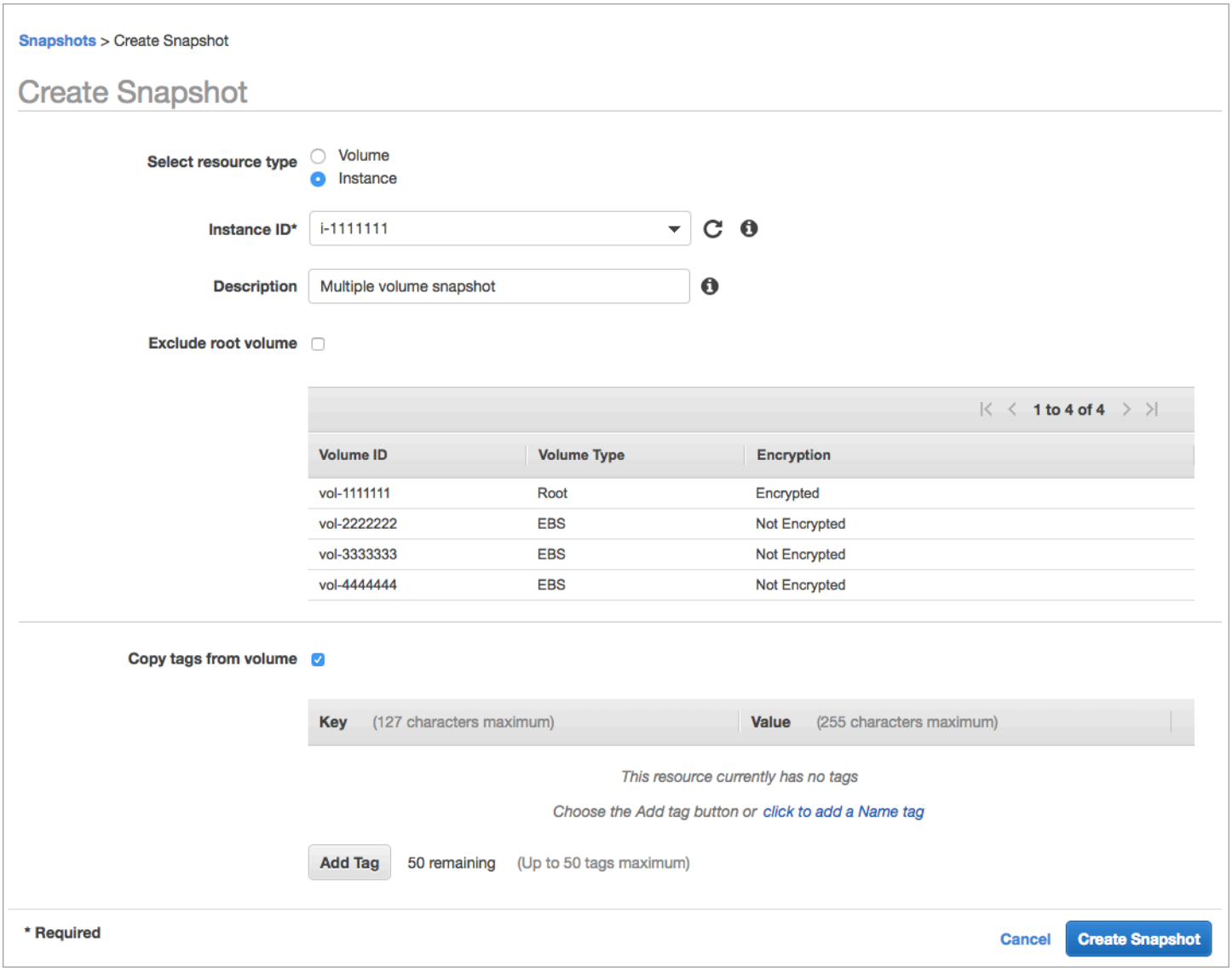
AWS Backup é exclusivo do Amazon Data Lifecycle Manager porque você pode criar um plano de backup que inclui recursos em vários serviços. AWS Você poderá coordenar seu backup para cobrir os recursos que você estiver usando juntos, em vez de coordenar os backups dos recursos individualmente.

AWS Backup também inclui o conceito de cofres de backup, que podem restringir o acesso aos pontos de recuperação dos backups concluídos. As operações de restauração podem ser iniciadas AWS Backup em vez de prosseguir com cada recurso individual e restaurar o backup criado. AWS Backup também inclui uma série de recursos adicionais, como gerenciamento de auditoria e relatórios. Para obter mais informações, consulte a seção Backup e recuperação usando AWS Backup desse guia.

## Execução de backups de vários volumes

Se você deseja fazer backup dos dados nos volumes do EBS em uma matriz RAID usando snapshots, os snapshots devem ser 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 sua matriz RAID, use a operação de CreateSnapshotsAPI ou faça login no console do Amazon EC2 e escolha Elastic Block Store, Snapshots, Create Snapshot.




Os instantâneos de instâncias que têm vários volumes conectados em uma configuração RAID são obtidos como instantâneos de vários volumes, coletivamente. Multi-volume os snapshots fornecem instantâneos pontuais, coordenados por 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 se obter consistência, pois os snapshots são tirados automaticamente em vários volumes do EBS. Após o snapshots dos volumes ser iniciado (geralmente um ou dois segundos), o sistema de arquivos poderá continuar suas operações.

Depois que os snapshots são criados, cada snapshot é tratado como um snapshot individual. Você pode realizar todas as operações de snapshot, como restaurar, excluir e copiar entre regiões e contas, assim como faria com um único snapshot de volume. Também 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. Para obter mais informações, consulte a documentação do AWS.

Você também poderá realizar esses backups a partir de um gerenciador de volumes lógicos ou de um backup em nível de sistema de arquivos. Nesses casos, o uso de um atendente de backup tradicional permite que os dados sejam copiados pela rede. Várias soluções de backup baseadas em atendente estão disponíveis na internet e no AWS Marketplace.

Uma abordagem alternativa é criar uma réplica dos volumes primários do sistema que existem em um único grande volume. Isso simplifica o processo de backup, pois é necessário fazer backup de apenas um grande volume, e o backup não ocorre no sistema primário. No entanto, primeiro determine se o volume único pode funcionar suficientemente durante o backup e se o tamanho máximo do volume é apropriado para o aplicativo.

## Proteção de seus backups do Amazon EC2

É importante considerar a segurança de seus backups e evitar a exclusão acidental ou maliciosa de seus backups. Você poderá utilizar várias abordagens coletivamente para fazer isso. Para evitar a perda de seus backups críticos devido a uma violação de segurança, recomendamos que você copie seus backups para outra AWS conta. Se você tiver várias AWS contas, poderá designar uma conta separada como sua conta de arquivamento para a qual todas as outras contas poderão copiar backups. Por exemplo, você pode fazer isso com um backup entre contas no AWS Backup.

Seu plano de recuperação de desastres também pode exigir que você seja capaz de reproduzir instâncias do EC2 em outra, Região da AWS no caso de uma falha regional. Você pode apoiar essa meta copiando seus backups para outra região dentro da mesma conta. Isso pode fornecer uma camada adicional de proteção contra exclusão acidental, bem como apoiar os objetivos de recuperação de desastres (DR). AWS Backup fornece suporte para backups entre regiões.

Considere bloquear as permissões do IAM para as ações ec2: DeleteSnapshot e ec2: DeregisterImage. Em vez disso, você poderá permitir que suas políticas e métodos de retenção gerenciem o ciclo de vida dos snapshots do EBS e das AMIs do Amazon EC2. Bloquear ações de exclusão é uma forma de implementar uma estratégia de escrever uma vez, ler muitos (WORM) em seus snapshots do EBS. Você também pode usar o AWS Backup Vault Lock, que fornece suporte para instantâneos do EBS e outros recursos. AWS

Além disso, considere bloquear a capacidade dos usuários de compartilhar AMIs e snapshots do EBS bloqueando as ações ec2: ModifyImageAttribute e ec2: IAM. ModifySnapshotAttribute Isso evitará que suas AMIs e snapshots sejam compartilhados com AWS contas externas à sua

organização. Se você estiver usando AWS Backup, limite os usuários de realizar operações semelhantes em cofres de backup. Para obter mais informações, consulte a seção AWS Backup desse guia.

O Amazon EBS inclui um atributo de lixeira que pode ajudá-lo a restaurar snapshots do EBS excluídos acidentalmente. Se você permitir que seus usuários excluam snapshots, ative esse atributo para que os snapshots necessários não sejam excluídos permanentemente. Os usuários devem ter cuidado especial ao excluir vários snapshots, porque o console do Amazon EC2 permite que você selecione vários snapshots e os exclua em uma operação. Além disso, tenha cuidado ao usar scripts de limpeza e automação para não excluir acidentalmente os snapshots dos quais precisa. O atributo Lixeira ajuda a fornecer proteção contra esses tipos de situações.

## Arquivamento de snapshots do EBS

Arquivar seus snapshots do EBS pode ser um método econômico para manter uma cópia de um volume para fins de referência que você não pretende restaurar por pelo menos 90 dias. Essa pode ser uma boa etapa intermediária antes de excluir permanentemente todos os snapshots relacionados de um volume do EBS. Por exemplo, você pode considerar o arquivamento de snapshots como uma etapa de fim do ciclo de vida para volumes do EBS que não são mais utilizados. Arquivar em vez de excluir também pode ser um método mais econômico de retenção de exclusões ao invés de usar a Lixeira.

## Automatizando a criação de instantâneos e AMI com o Systems Manager, o AWS CLI, e o AWS SDKs

Sua abordagem de backup pode exigir operações antes e depois da criação de um snapshot ou AMI. Por exemplo, talvez seja necessário interromper e iniciar serviços para desativar o sistema de arquivos. Ou talvez você precise interromper e iniciar sua instância durante a criação da AMI. Talvez você também precise criar backups de vários componentes em sua arquitetura coletivamente, cada um com suas próprias etapas de pré-criação e pós-criação.

Você pode reduzir o tempo de manutenção dos backups automatizando o processo e verificando se o processo de backup é aplicado de forma consistente. Para automatizar suas operações personalizadas de pré-criação e pós-criação, crie um script para seu processo de backup usando o AWS CLI e o SDK.

Sua automação pode ser definida em um runbook do Systems Manager que pode ser executado sob demanda ou durante uma janela de manutenção do Systems Manager. Você pode conceder

aos seus usuários acesso para executar runbooks do Systems Manager sem a necessidade de conceder a eles permissões para comandos disruptivos do Amazon EC2. Isso também pode ajudá-lo a verificar se o processo de backup e as tags são aplicados de forma consistente pelos usuários. Você pode usar os AWS- CreateSnapshot e AWS- CreateImage runbooks para criar instantâneos e AMIs, ou você pode conceder a outros usuários permissões para usá-los. O Systems Manager também inclui os AWS- UpdateLinuxAmi e AWS- UpdateWindowsAmi runbooks para automatizar a aplicação de patches e a criação de AMI.

Você também pode usar o AWS CLI e AWS Tools for Windows PowerShellpara automatizar seu processo de criação de instantâneos e AMI. Você pode usar o AWS CLI comando aws ec2 create-snapshot para criar um instantâneo de um volume do EBS como uma etapa da sua automação. Você pode usar o comando aws ec2 create-snapshots para criar snapshots sincronizados e consistentes em caso de falhas de todos os volumes conectados à sua instância do EC2.

Você pode usar a AWS CLI para criar novas AMIs. Você pode usar o comando aws ec2 register-image para criar uma nova imagem para sua instância do EC2. Para automatizar o desligamento, a criação de imagens e a reinicialização de suas instâncias, combine esse comando com os comandos aws ec2 stop-instances e aws ec2 start-instances.

## Restauração de um volume do Amazon EBS ou uma instância do EC2

Se você precisar restaurar apenas um único volume conectado a uma instância do EC2, poderá restaurar esse volume separadamente, desanexar o volume existente e anexar o volume restaurado à sua instância do EC2. Se você precisar restaurar uma instância EC2 inteira, incluindo todos os volumes associados, deverá usar um backup da Imagem de máquina da Amazon (AMI) da sua instância.

Para reduzir o tempo de recuperação e o impacto nos aplicativos e processos dependentes, seu processo de restauração deve considerar o recurso que está substituindo. Para obter melhores resultados, teste regularmente o processo de restauração em ambientes inferiores (por exemplo, sem produção) para verificar se o processo atende ao objetivo de ponto de recuperação (RPO) e ao objetivo de tempo de recuperação (RTO) e se o processo de restauração funciona conforme o esperado. Considere como o processo de restauração afetará os aplicativos e serviços que dependem da instância que você está restaurando e, em seguida, coordene a restauração conforme necessário. Tente automatizar e testar o processo de restauração o máximo possível para reduzir o risco de seu processo de restauração falhar ou ser implementado de forma inconsistente.

Se você utilizar o balanceador de carga elástico, com várias instâncias atendendo ao tráfego, você pode tirar de serviço uma instância com falha ou com defeito. Em seguida, você pode restaurar uma nova instância para substituí-la enquanto as outras instâncias continuam atendendo ao tráfego sem interromper os usuários.

Os seguintes processos de restauração descritos são para instâncias que não estão usando balanceador de carga estático:

- Restauração de arquivos e diretórios individuais a partir de snapshots do EBS
- Restauração de um volume do EBS a partir de um snapshot do Amazon EBS
- Criação ou restauração de uma instância EC2 a partir de um snapshot do EBS
- Restauração de uma instância em execução a partir de uma AMI

## Restauração de arquivos e diretórios a partir de snapshots do EBS

Os snapshots do EBS fornecem uma réplica exata do volume original usado para criar o snapshot. Para restaurar arquivos ou diretórios individuais, você deve fazer o seguinte:

1. Primeiro, restaure o volume do snapshot do EBS que contém os arquivos ou diretórios.
2. Anexe o volume à instância do EC2 na qual você deseja restaurar os arquivos.
3. Copie os arquivos do volume restaurado para o volume da sua instância do EC2.
4. Separe e exclua o volume restaurado.

## Restauração de um volume do EBS a partir de um snapshot do Amazon EBS

Você pode restaurar um volume anexado a uma instância EC2 existente criando um volume a partir do snapshot e anexando-o à sua instância. Você pode usar o console, o AWS CLI, ou as operações da API para criar um volume a partir de um snapshot existente. Em seguida, você pode montar o volume na instância usando o sistema operacional.

Observe que os dados de um snapshot do Amazon EBS são carregados de forma assíncrona em um volume do EBS. Se um aplicativo acessar o volume no qual os dados não estão carregados, haverá uma latência maior do que o normal enquanto os dados forem carregados do Amazon S3. Para evitar esse impacto para aplicativos sensíveis à latência, você tem duas opções:

- Você pode inicializar o volume do EBS.
- Por uma taxa adicional, o Amazon EBS oferece suporte à restauração rápida de snapshots, o que elimina a necessidade de inicializar seu volume.

Se você estiver substituindo um volume que deve usar o mesmo ponto de montagem, desmonte esse volume para poder montar o novo volume em seu lugar. Para desmontar o volume, primeiro interrompa todos os processos que estão usando o volume. Se estiver substituindo o volume raiz, você deverá interromper a instância primeiro antes de separar o volume raiz.

Por exemplo, siga estas etapas para restaurar um volume para um backup point-in-time anterior usando o console:

1. No console do Amazon EC2, no menu Elastic Block Store, escolha Snapshots.
2. Procure o snapshot que deseja restaurar e selecione-o.
3. Escolha Ações e, em seguida, selecione Criar volume.
4. Crie um novo volume do na mesma zona de disponibilidade de sua instância EC2.
5. No console do Amazon EC2, selecione a instância.
6. Nos detalhes da instância, anote o nome do dispositivo que você deseja substituir nas entradas Dispositivo raiz ou Dispositivos de blocos.
7. Anexe o volume. O processo é diferente para volumes raiz e volumes não raiz.

   Para volumes raiz:

   a. Pare a instância do EC2.
   b. No menu Volumes EC2 Elastic Block Store, selecione o volume raiz que você deseja substituir.
   c. Escolha Actions (Ações) e Detach Volume (Desvincular volume).
   d. No menu Volumes EC2 Elastic Block Store, selecione o novo volume.
   e. Escolha Actions (Ações) e Attach Volume (Anexar volume).
   f. Selecione a instância à qual você deseja conectar o volume e use o mesmo nome de dispositivo que você anotou anteriormente.

   Para volumes não raiz:

   a. No menu Volumes EC2 Elastic Block Store, selecione o volume não raiz que você deseja substituir.
   b. Escolha Actions (Ações) e Detach Volume (Desvincular volume).

c. Anexe o novo volume escolhendo-o no menu Volumes EC2 Elastic Block Store e, em seguida, escolhendo Ações, Anexar volume. Selecione a instância à qual você deseja anexar e, em seguida, selecione um nome de dispositivo disponível.

d. Usando o sistema operacional da instância, desmonte o volume existente e, em seguida, monte o novo volume em seu lugar.

   No Linux, você pode usar o comando `umount`. No Windows, você pode usar um gerenciador de volume lógico (LVM), como o utilitário do sistema de gerenciamento de disco.

e. Separe quaisquer volumes anteriores que você possa estar substituindo escolhendo-os no menu Volumes EC2 Elastic Block Store e, em seguida, escolhendo Ações, Desanexar volume.

Você também pode usar o AWS CLI em combinação com os comandos do sistema operacional para automatizar essas etapas.

## Criação ou restauração de uma instância EC2 a partir de um snapshot do EBS

Para criar um backup que será utilizado para restaurar uma instância do EC2 inteira, recomendamos criar uma Imagem de máquina da Amazon (AMI). As AMIs capturam informações da máquina, como o tipo de virtualização. Eles também criam snapshots para cada volume conectado à instância do EC2, incluindo seus mapeamentos de dispositivos, para que possam ser restaurados na mesma configuração.

> **Note**
>
> Na maioria dos casos, as AMIs para Windows, Red Hat, SUSE e SQL Server exigem que as informações corretas de licenciamento estejam presentes na AMI. Para obter mais informações, consulte Entender as informações de faturamento da AMI. Ao criar uma AMI de um snapshot, a operação `RegisterImage` obtém as informações de faturamento corretas dos metadados do snapshot, mas isso exige que os metadados apropriados estejam presentes. Para verificar se as informações de cobrança corretas foram aplicadas, verifique o campo Detalhes da plataforma na nova AMI. Se o campo estiver vazio ou não corresponder ao código do sistema operacional esperado (por exemplo, Windows, Red Hat, SUSE ou SQL), a criação da AMI não foi bem-sucedida e você deve descartar a AMI e seguir as instruções em Criar uma AMI a partir de uma instância.

Se você precisar usar um snapshot do EBS para restaurar uma instância, primeiro crie uma AMI a partir de um snapshot do EBS que se tornará o volume raiz da sua nova instância do EC2:

1. No console do Amazon EC2, no menu Elastic Block Store, escolha Snapshots.
2. Procure o snapshot que será utilizado para criar o volume raiz para sua nova instância do EC2 e selecione-o.
3. Selecione Actions (Ações), e. em seguida, Create Image (Criar imagem).
4. Insira um nome para sua imagem (por exemplo, `YYYYMMDD-restore-for-i-012345678998765de`) e escolha as opções apropriadas para sua nova imagem.
5. (Somente para Windows, Red Hat, SUSE e SQL Server) Para verificar se as informações de cobrança corretas foram aplicadas, verifique o campo Detalhes da plataforma na nova AMI. Se o campo estiver vazio ou não corresponder ao código esperado do sistema operacional (por exemplo, Windows ou Red Hat), a criação da AMI não teve êxito e você deverá descartá-la e seguir as instruções em Criar uma AMI a partir de uma instância.

Após a imagem ser criada e disponibilizada, você poderá iniciar uma nova instância do EC2 que usará o snapshot do EBS para o volume raiz.

## Restauração de uma instância em execução a partir de uma AMI

Você pode abrir uma nova instância do backup da AMI para substituir uma instância existente em execução. Uma abordagem é interromper a instância existente, mantê-la off-line enquanto você executa uma nova instância a partir da sua AMI e realizar as atualizações necessárias. Essa abordagem reduz o risco de conflitos de ambas as instâncias em execução simultânea. É uma abordagem aceitável se os serviços que sua instância fornece estiverem inativos ou se você estiver executando a restauração durante uma janela de manutenção. Após testar sua nova instância, você poderá reatribuir qualquer endereço IP elástico que tenha sido alocado para a instância antiga. Em seguida, você pode atualizar qualquer registro do Serviço de Nomes de Domínio (DNS) para apontar para a nova instância.

No entanto, se durante uma restauração você precisar minimizar o tempo de inatividade da sua instância em serviço, considere iniciar e testar uma nova instância a partir do backup da AMI. Em seguida, substitua a instância existente pela nova instância.

Enquanto as duas instâncias estiverem em execução, você deve evitar que a nova instância cause colisões no nível da plataforma ou do aplicativo. Por exemplo, você pode ter problemas com instâncias do Windows associadas ao domínio que estão sendo executadas com os mesmos SIDs

e nome de computador. Você pode encontrar problemas semelhantes com aplicativos e serviços de rede que exigem identificadores exclusivos.

Para evitar que outros servidores e serviços se conectem à sua nova instância antes que ela esteja pronta, use grupos de segurança para bloquear temporariamente todas as conexões de entrada da sua nova instância, exceto seu próprio endereço IP para acesso e teste. Você também pode bloquear temporariamente as conexões de saída da nova instância para impedir que serviços e aplicativos iniciem conexões ou atualizações de outros recursos. Quando a nova instância estiver pronta, interrompa a instância existente, inicie serviços e processos na nova instância e, em seguida, desbloqueie todas as conexões de rede de entrada ou saída que você implementou.

# Backup e recuperação da infraestrutura local para AWS

Você pode usar AWS para armazenamento externo durável de seus backups de infraestrutura local. Ao usar serviços AWS de armazenamento nesse cenário, você pode se concentrar nas tarefas de backup e arquivamento. Você não precisa se preocupar com o provisionamento, o dimensionamento ou a capacidade da infraestrutura de armazenamento para suas tarefas de backup.

O Amazon S3 oferece operações API abrangentes e SDKs para integração em suas abordagens de backup e recuperação novas e existentes. Isso também oferece aos fornecedores de software de backup formas de integrar diretamente seus aplicativos às soluções AWS de armazenamento.

Nesse cenário, o software de backup e arquivamento que você está usando em sua infraestrutura local interage diretamente por AWS meio das operações de API. Como o software de backup AWS reconhece, ele faz backup dos dados dos servidores locais diretamente no Amazon S3.

Se seu software de backup existente não oferecer suporte nativo à AWS nuvem, você poderá usar o Storage Gateway. Um serviço de armazenamento em nuvem, o Storage Gateway dá aos seus sistemas on-premises acesso ao armazenamento em nuvem escalável. Ele suporta protocolos de armazenamento de padrão aberto que funcionam com seus aplicativos existentes enquanto armazenam com segurança seus dados criptografados no Amazon S3. Você pode usar o Storage Gateway como parte de uma abordagem de backup e recuperação para suas workloads de armazenamento on-premises baseadas em blocos.

O Storage Gateway é útil em cenários híbridos em que você deseja fazer a transição para o armazenamento baseado em nuvem para seus backups. O Storage Gateway também ajuda a reduzir os investimentos de capital em armazenamento on-premises. Você implanta o Storage Gateway como uma VM ou um dispositivo de hardware dedicado. Este guia se concentra em como o Storage Gateway se aplica ao backup e à recuperação.

O Storage Gateway oferece três opções diferentes para atender a diferentes requisitos:

- Um gateway de arquivos para armazenar arquivos de dados de aplicativos e imagens de backup como objetos duráveis no armazenamento em nuvem do Amazon S3 usando SMB-based ou NFS-based acessando.
- Um gateway de volumes para apresentar volumes de armazenamento em blocos iSCSI baseados em nuvem para suas aplicações on-premises. Um gateway de volumes fornece um cache local ou volumes completos on-premises, além de armazenar cópias completas de seus volumes na AWS Cloud.

- Um gateway de fitas para direcionar um software de backup confiável para um gateway de armazenamento on-premises que, por sua vez, se conecta ao Amazon S3. Essa opção oferece a escala e a durabilidade da nuvem para retenção segura e de longo prazo sem interromper os investimentos ou processos existentes.

## Gateway de arquivos

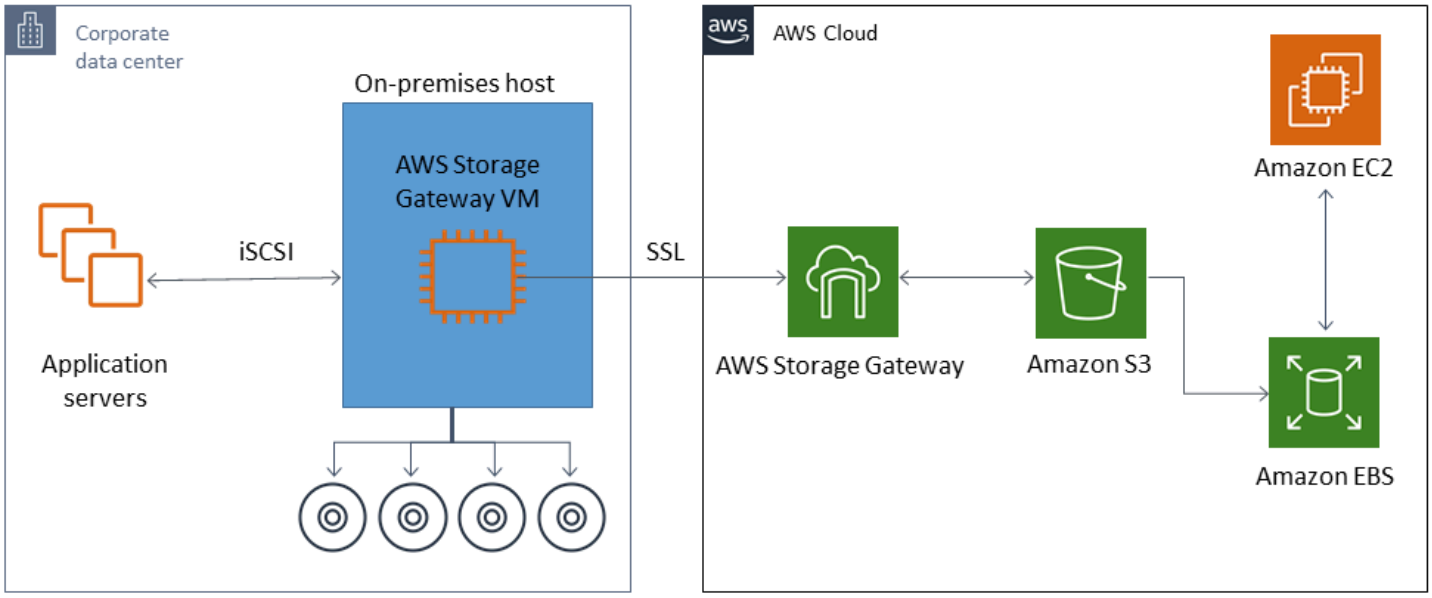
Muitas organizações iniciam sua jornada para a nuvem transferindo dados secundários e terciários, como backups, para a nuvem. O suporte à interface SMB e NFS de um gateway de arquivos fornece uma maneira de os grupos de TI fazerem a transição das tarefas de backup dos sistemas de backup on-premises existentes para a nuvem. Aplicativos de backup, ferramentas nativas de banco de dados ou scripts que podem gravar em SMB ou NFS podem gravar em um gateway de arquivos. O gateway de arquivos armazena os backups como objetos do Amazon S3 de até 5 TiB de tamanho. Com um cache local de tamanho adequado, os backups recentes podem ser usados para recuperações rápidas no local. Long-term as necessidades de retenção são atendidas por meio da hierarquização dos backups em classes de armazenamento S3 Standard-Infrequent Access e Amazon Glacier de baixo custo.

O gateway de arquivos fornece uma rampa de acesso para seu armazenamento baseado em blocos no Amazon S3 para backups externos altamente duráveis. É especialmente útil para cenários em que um arquivo de backup recente deve ser restaurado rapidamente. Como um gateway de arquivos suporta os protocolos SMB e NFS, os usuários podem acessar arquivos da mesma forma que acessariam um compartilhamento de arquivos de rede. Você também pode utilizar os recursos de controle de versionamento de objetos do Amazon S3. Usando o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos de um arquivo e acessá-las facilmente usando SMB ou NFS.

## Gateway de volumes

Um gateway de volumes permite que você provisione volumes de armazenamento em blocos iSCSI baseados em nuvem para seus servidores on-premises. O gateway de volumes armazena seus dados de volume no Amazon S3 para armazenamento externo durável e escalável baseado em nuvem. Um gateway de volumes facilita a captura de snapshots point-in-time completos de seus volumes e o armazenamento deles na nuvem como snapshots do Amazon EBS. Depois de serem armazenados como snapshots, volumes inteiros podem ser restaurados como volumes do EBS e anexados às instâncias do EC2, acelerando uma solução de DR baseada em nuvem. Os volumes

também podem ser restaurados no Storage Gateway, permitindo que seus aplicativos on-premises voltem ao estado anterior.



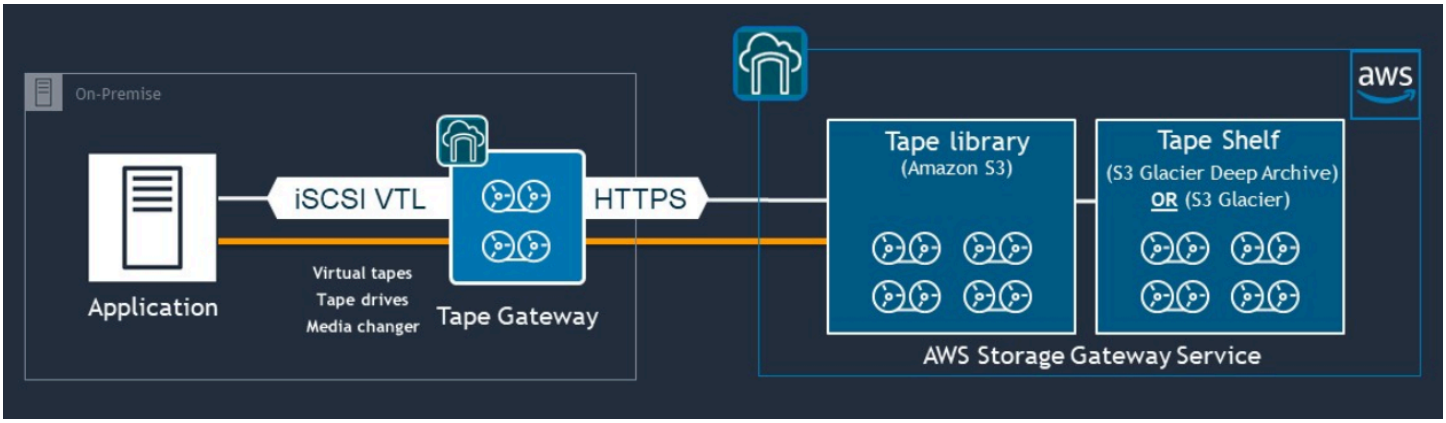

Como um gateway de volume se integra ao recurso de volume Amazon EBS do Amazon EC2, você pode AWS Backup usá-lo para automatizar e programar seu processo de snapshot. Um gateway de volumes oferece a você os benefícios adicionais de snapshot e atributos de marcação duráveis do Amazon EBS com suporte do Amazon S3. Para obter mais informações, consulte a documentação de snapshot do Amazon EBS.

## Gateway de fitas

Um gateway de fitas oferece armazenamento hierárquico de alta durabilidade e baixo custo, e atributos abrangentes do Amazon S3 para seu armazenamento de backup em fita virtual externo. Todas as suas fitas virtuais armazenadas no Amazon S3 são replicadas e armazenadas em pelo menos três zonas de disponibilidade geograficamente dispersas. Suas fitas virtuais são protegidas por 11 noves de durabilidade.

AWS também realiza verificações de fixidez regularmente para confirmar que seus dados podem ser lidos e que nenhum erro foi introduzido. Todas as fitas armazenadas no Amazon S3 são protegidas por criptografia do lado do servidor usando chaves padrão ou suas chaves. AWS KMS Além disso, você evita riscos de segurança física associados à portabilidade de fitas. Com um gateway de fitas, você obtém os dados corretos em comparação com o armazenamento de fitas externo, onde você pode receber uma fita incorreta ou quebrada durante a restauração.

Você pode economizar nos custos mensais de armazenamento ao armazenar seus dados no Amazon S3. Você pode economizar ainda mais para seus requisitos de arquivamento de longo prazo usando o S3 Glacier Deep Archive.




Um gateway de fitas atua como uma biblioteca virtual de fitas (VTL) que abrange desde seu ambiente on-premises até serviços de armazenamento altamente escaláveis, redundantes e duráveis: Amazon S3, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

O gateway de fita apresenta o Storage Gateway ao seu aplicativo de backup existente como um padrão aberto i SCSI-based VTL, com um trocador de mídia virtual e unidades de fita virtuais. Você pode continuar usando seus aplicativos e fluxos de trabalho de backup existentes enquanto grava em uma coleção de fitas virtuais armazenadas no Amazon S3 altamente escalável. Quando você não precisar mais de acesso imediato ou frequente aos dados em uma fita virtual, seu aplicativo de backup pode arquivá-los no S3 Glacier Flexible Retrieval ou no S3 Glacier Deep Archive, reduzindo ainda mais os custos de armazenamento.

Você pode recuperar uma fita arquivada na opção S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive normalmente em 3 a 5 horas ou 12 horas, respectivamente. O gateway de fitas pode ser usado com um aplicativo de backup compatível com a interface i SCSI-based tape library para acessar as fitas virtuais. Considere também o tamanho mínimo de armazenamento de 100 GB por fita. Para obter mais informações, consulte a lista de aplicativos de backup de terceiros que oferecem suporte a gateways de fitas.

# Backup e recuperação de aplicativos da AWS para o seu datacenter

Você pode ter uma política exigindo que você implemente um cenário como DR ou continuidade de negócios para seus workloads baseados na nuvem e sua infraestrutura on-premises. Se você já tem uma estrutura de backup de dados para seus servidores on-premises, pode estendê-la aos seus recursos da AWS por meio de uma conexão VPN ou por meio do AWS Direct Connect. Você pode instalar o atendente de backup nas instâncias do EC2 e fazer backup de seus dados e aplicativos de acordo com suas políticas de proteção de dados. Você também pode usar o Amazon S3 como serviço intermediário para armazenar seus backups em nível de aplicativo. Em seguida, você pode usar as operações de API, os SDKs ou a AWS CLI para restaurar os dados em seu ambiente on-premises.

Para fazer backup de dados em serviços AWS que não sejam o Amazon EC2, use o AWS CLI, os SDKs e as operações de API para extrair os dados no formato desejado. Em seguida, copie os dados para o Amazon S3, e copie-os do Amazon S3 para seu ambiente on-premises. Alguns serviços fornecem exportação direta para o Amazon S3. Por exemplo, o Amazon RDS oferece suporte ao backup nativo de bancos de dados Microsoft SQL Server para o Amazon S3.

# Backup e recuperação de serviços nativos em nuvem AWS

Sua abordagem de backup e recuperação deve abranger os AWS serviços usados em suas cargas de trabalho. AWS fornece recursos e opções específicos do serviço para gerenciar e interagir com seus dados. Você pode usar o console, o AWS CLI SDKs, e as operações de API para implementar backup e recuperação para os AWS serviços que você está usando. Este guia aborda o Amazon RDS e o Amazon DynamoDB como exemplos. O AWS Backup oferece suporte ao DynamoDB e ao Amazon RDS e deve ser usado se atender aos seus requisitos.

## Backup e recuperação para o Amazon RDS

O Amazon RDS inclui recursos para automatizar backups de bancos de dados. O Amazon RDS cria um snapshot do volume de armazenamento de sua instância de banco de dados, fazendo o backup de toda a instância de banco de dados, não apenas dos bancos de dados individuais. Usando o Amazon RDS, você pode estabelecer uma janela de backup para backups automatizados, criar instantâneos de instâncias de banco de dados e compartilhar e copiar instantâneos entre regiões e contas.

O Amazon RDS oferece duas opções diferentes para fazer backup e restaurar suas instâncias de banco de dados:

- Os backups automatizados fornecem point-in-time recuperação (PITR) da sua instância de banco de dados. Backup automatizado é ativado por padrão quando você cria uma instância de banco de dados.

  O Amazon RDS realiza um backup diário dos seus dados durante uma janela de backup que você define ao criar a instância de banco de dados. Você pode configurar o período de retenção de backup automático para até 35 dias. O RDS faz upload dos logs de transações de instâncias de banco de dados no Amazon S3 a cada cinco minutos. O Amazon RDS usa seus backups diários junto com seus registros de transações do banco de dados para restaurar sua instância de banco de dados. Você pode restaurar a instância a qualquer segundo durante o período de retenção, até `LatestRestorableTime` (normalmente, os últimos cinco minutos).

  Para descobrir o horário restaurável mais recente para suas instâncias de banco de dados, use a chamada de API do `DescribeDBInstances`. Ou procure na guia Descrição o banco de dados no console do Amazon RDS.

Quando você inicia uma PITR, os registros de transações são combinados com o backup diário mais adequado para restaurar sua instância de banco de dados no horário solicitado.

- Os snapshots de banco de dados são backups iniciados pelo usuário que você pode usar para restaurar a sua instância do BD em um estado conhecido como desejar. Em seguida, você pode restaurar esse estado a qualquer momento. Você pode usar o console do Amazon RDS ou a chamada de API do `CreateDBSnapshot` para criar snapshots de banco de dados. Esses instantâneos são mantidos até que você use o console ou a chamada de API do `DeleteDBSnapshot` para excluí-los explicitamente.

Ambas as opções de backup são suportadas pelo Amazon RDS in AWS Backup, que também fornece outros recursos. Considere usar AWS Backup para configurar um plano de backup padrão para seus bancos de dados Amazon RDS e use as opções de backup de instância iniciadas pelo usuário quando seus planos de backup para um banco de dados específico forem exclusivos.

O Amazon RDS impede o acesso direto ao armazenamento subjacente usado pela instância de banco de dados. Isso também impede que você exporte diretamente o banco de dados em uma instância de banco de dados do RDS para seu disco local. Em alguns casos, você pode usar funções nativas de backup e restauração usando utilitários de cliente. Por exemplo, você pode usar o comando mysqldump com um banco de dados MySQL do Amazon RDS para exportar um banco de dados para sua máquina cliente local. Em alguns casos, o Amazon RDS também fornece opções aumentadas para realizar um backup e restauração nativos de um banco de dados. Por exemplo, o Amazon RDS fornece procedimentos armazenados para exportar e importar backups de bancos de dados RDS de bancos de dados SQL Server.

Certifique-se de testar minuciosamente o processo de restauração do banco de dados e seu impacto nos clientes do banco de dados como parte de sua abordagem geral de backup e restauração.

## Usando registros DNS CNAME para reduzir o impacto no cliente durante a recuperação do banco de dados

Quando você restaura um banco de dados usando PITR ou um snapshot de instância de banco de dados do RDS, uma nova instância de banco de dados com um novo endpoint é criada. Dessa forma, você pode criar várias instâncias de banco de dados a partir de um DB snapshot ou point-in-time específico. Há considerações especiais ao restaurar uma instância de banco de dados do RDS para substituir uma instância de banco de dados ativa do RDS. Por exemplo, você deve determinar como redirecionará seus clientes de banco de dados existentes para a nova instância com o mínimo

de interrupção e modificação. Você também deve garantir a continuidade e a consistência dos dados no banco de dados considerando o tempo de restauração dos dados e o tempo de recuperação quando a nova instância começa a receber gravações.

Você pode criar um registro DNS CNAME separado que aponta para o endpoint da sua instância de banco de dados e fazer com que seus clientes usem esse nome DNS. Em seguida, você pode atualizar o CNAME para apontar para um novo endpoint restaurado sem precisar atualizar seus clientes de banco de dados.

Defina o tempo de vida (TTL) do seu registro CNAME com um valor apropriado. O TTL que você especifica determina por quanto tempo o registro é armazenado em cache com resolvedores de DNS antes que outra solicitação seja feita. É importante observar que alguns resolvedores ou aplicativos de DNS podem não respeitar o TTL e podem armazenar o registro em cache por mais tempo do que o TTL. Para o Amazon Route 53, se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para obter mais informações, consulte Como o Amazon Route 53 roteia o tráfego para seu domínio.

Aplicativos e sistemas operacionais clientes também podem armazenar em cache as informações de DNS que você precisa limpar ou reiniciar para iniciar uma nova solicitação de resolução de DNS e recuperar o registro CNAME atualizado.

Ao iniciar uma restauração do banco de dados e transferir o tráfego para a instância restaurada, verifique se todos os seus clientes estão gravando na instância restaurada em vez da instância anterior. Sua arquitetura de dados pode oferecer suporte à restauração do banco de dados, à atualização do DNS para transferir o tráfego para a instância restaurada e, em seguida, à correção de quaisquer dados que ainda possam estar gravados na instância anterior. Se esse não for o caso, você pode interromper sua instância existente antes de atualizar o registro DNS CNAME. Então, todo o acesso é da sua instância recém-restaurada. Isso pode causar temporariamente problemas de conexão para alguns de seus clientes de banco de dados, que você pode manipular individualmente. Para reduzir o impacto no cliente, você pode executar a restauração do banco de dados durante uma janela de manutenção.

Escreva seus aplicativos para lidar com falhas de conexão de banco de dados normalmente com novas tentativas usando o recuo exponencial. Isso permite que seu aplicativo se recupere quando uma conexão de banco de dados fica indisponível durante uma restauração sem causar uma falha inesperada no aplicativo.

Depois de concluir o processo de restauração, você pode manter sua instância anterior em um estado interrompido. Ou você pode usar as regras do grupo de segurança para limitar o tráfego para sua instância anterior até ter certeza de que ela não é mais necessária. Para uma abordagem de descomissionamento gradual, primeiro limite o acesso a um banco de dados em execução pelo grupo de segurança. Eventualmente, você poderá interromper a instância quando ela não for mais necessária. Por fim, tire um instantâneo da instância do banco de dados e exclua-o.

## Backup e recuperação para o DynamoDB

O DynamoDB fornece PITR, que faz backups quase contínuos dos dados de tabelas do DynamoDB. Quando habilitado, o DynamoDB mantém backups incrementais de sua tabela nos últimos 35 dias até que você o desative explicitamente.

Você também pode criar backups sob demanda da sua tabela do DynamoDB usando o console do DynamoDB, o ou a API do DynamoDB. AWS CLI Para obter mais informações, consulte Como fazer backup de uma tabela do DynamoDB. Você pode programar backups periódicos ou futuros usando AWS Backup, ou você pode personalizar e automatizar sua abordagem de backup usando funções Lambda. Para obter mais informações, veja a postagem do blog Uma solução com tecnologia sem servidor para agendar o backup sob demanda do Amazon DynamoDB. Se você não quiser criar scripts de agendamento e trabalhos de limpeza, você pode usar AWS Backup para criar planos de backup. Os planos de backup incluem agendas e políticas de retenção para suas tabelas do DynamoDB. AWS Backup cria os backups e exclui os backups anteriores com base no seu cronograma de retenção. AWS Backup também inclui opções avançadas de backup do DynamoDB que não estão disponíveis no serviço do DynamoDB, incluindo armazenamento hierárquico de baixo custo e cópia entre contas e regiões. Para obter mais informações, consulte Backup avançado do DynamoDB.

Você deve configurar manualmente os itens a seguir na tabela restaurada:

- Políticas de escalabilidade automática
- Políticas do IAM
- CloudWatch Métricas e alarmes da Amazon
- Tags
- Configurações de fluxo
- Configurações de (TTL)

Só é possível restaurar os dados completos da tabela para uma nova tabela por meio de backup. Você pode gravar na tabela restaurada somente depois que ela fica ativa.

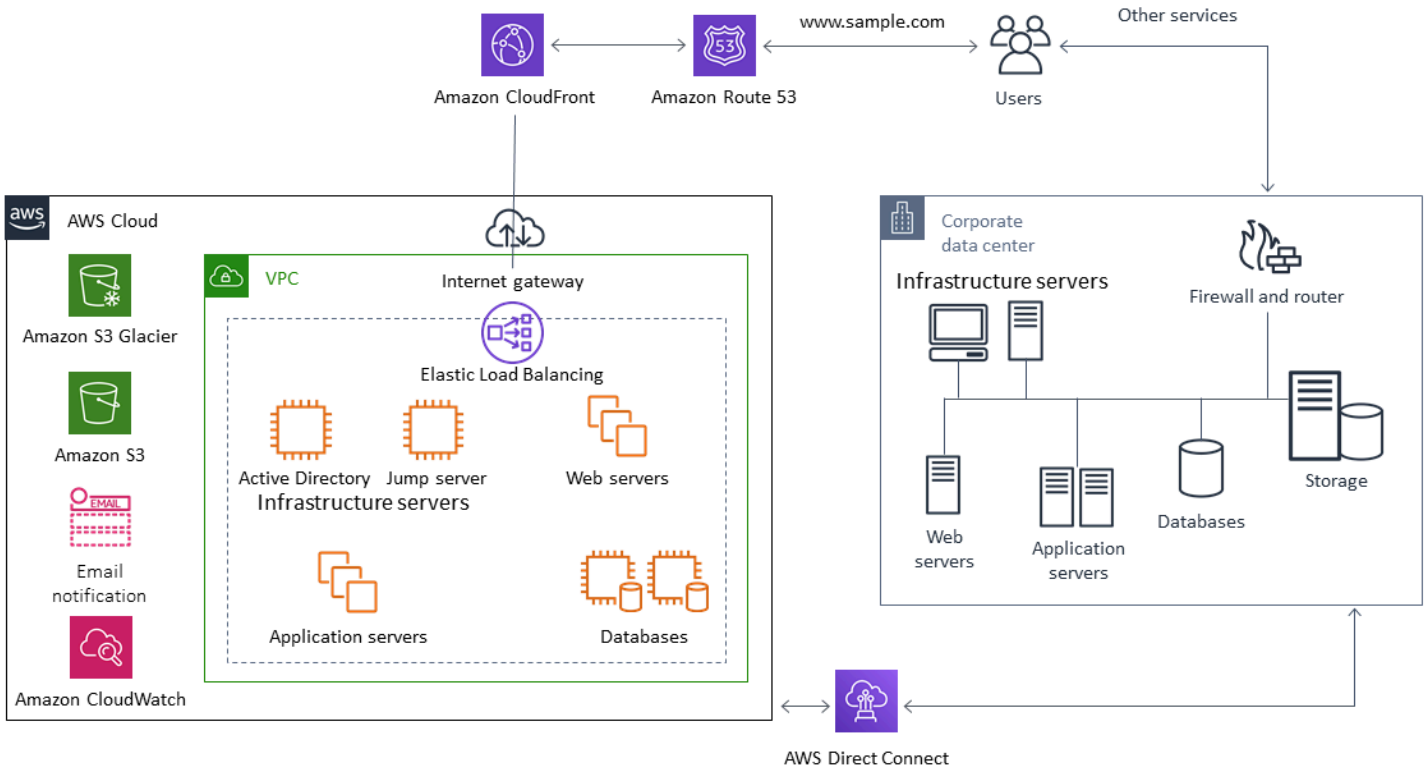
Seu processo de restauração deve considerar como os clientes serão orientados a usar o nome da tabela recém-restaurada. Você pode configurar seus aplicativos e clientes para recuperar o nome da tabela do DynamoDB de um arquivo de configuração AWS Systems Manager , valor do Parameter Store ou outra referência que possa ser atualizada dinamicamente para refletir o nome da tabela que o cliente deve usar.

Como parte do processo de restauração, você deve considerar cuidadosamente o processo de troca. Você pode optar por negar o acesso à sua tabela existente do DynamoDB por meio das permissões do IAM e permitir o acesso à sua nova tabela. Em seguida, você pode atualizar a configuração do aplicativo e do cliente para usar a nova tabela. Talvez você também precise reconciliar as diferenças entre sua tabela atual do DynamoDB e a tabela do DynamoDB recém-restaurada.

# Backup e recuperação para arquiteturas híbridas

As implantações locais e nativas da nuvem discutidas neste guia podem ser combinadas em cenários híbridos em que o ambiente de carga de trabalho tem componentes locais e de infraestrutura. AWS Os recursos, incluindo servidores web, servidores de aplicativos, servidores de monitoramento, bancos de dados e o Microsoft Active Directory, são hospedados no data center do cliente ou na AWS. Os aplicativos que estão sendo executados na AWS nuvem são conectados aos aplicativos que estão sendo executados no local.

Isso está se tornando um cenário comum para workloads corporativas. Muitas empresas têm data centers próprios e os usam AWS para aumentar a capacidade. Esses data centers de clientes geralmente são conectados à AWS rede por links de rede de alta capacidade. Por exemplo, com Direct Connect, você pode estabelecer conectividade privada e dedicada do seu data center local para o. AWS Isso fornece a largura de banda e a latência consistente para carregar dados na nuvem para fins de proteção de dados. Ele também fornece desempenho e latência consistentes para workloads híbridas. O diagrama a seguir fornece um exemplo de uma abordagem de ambiente híbrido.




Well-designed as soluções de proteção de dados geralmente usam uma combinação das opções descritas nas soluções nativas da nuvem e locais neste guia. Muitos ISVs fornecem soluções de

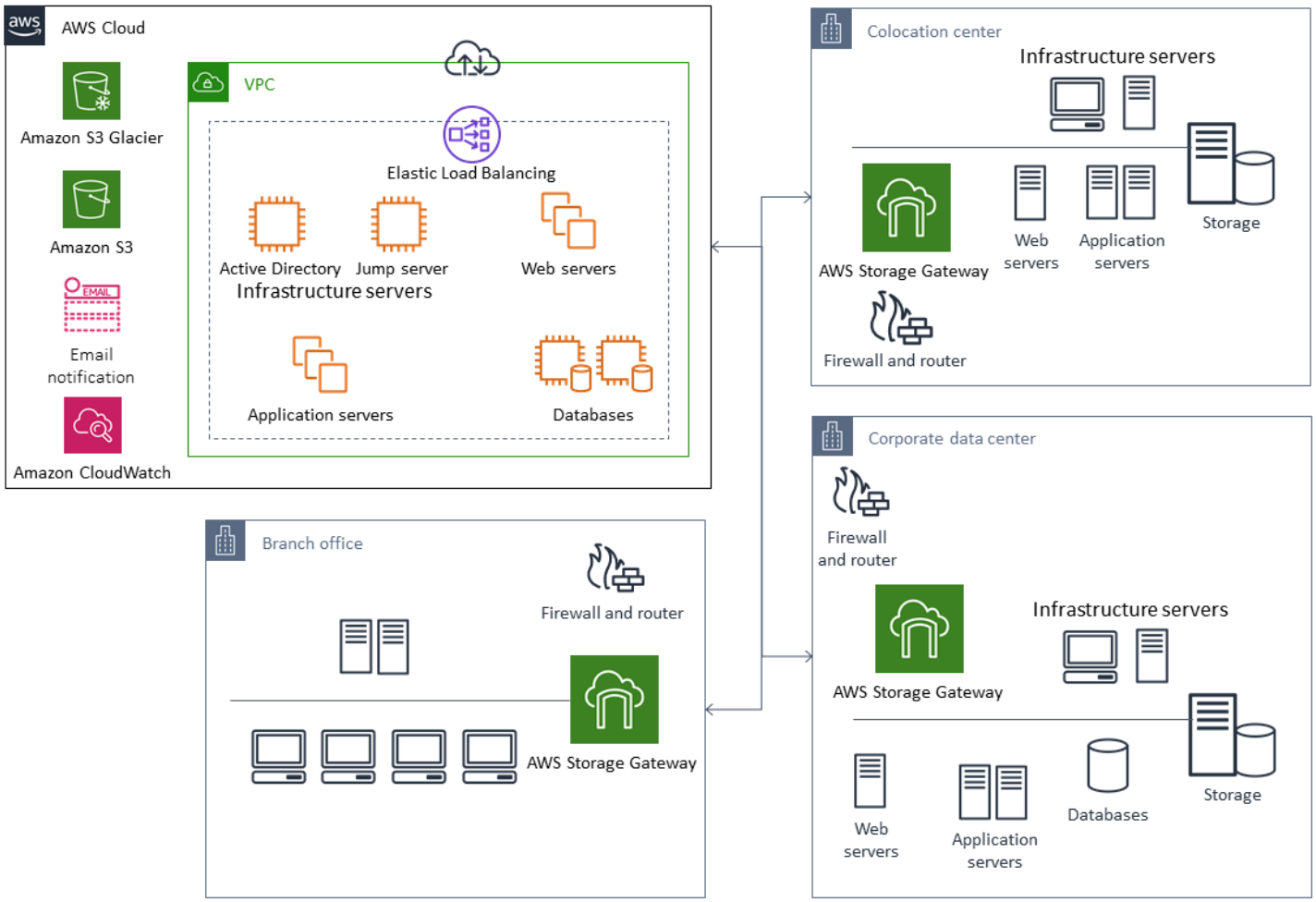
backup e restauração líderes de mercado para infraestrutura on-premises e expandiram suas soluções para oferecer suporte a abordagens híbridas.

## Mover soluções centralizadas de gerenciamento de backup para a nuvem para maior disponibilidade

Ao usar seus investimentos existentes em soluções de gerenciamento de backup com AWS, você pode melhorar a resiliência e a arquitetura de sua abordagem. Você pode ter um servidor de backup primário e um ou mais servidores de mídia ou armazenamento localizados on-premises em vários locais próximos aos servidores e serviços que eles estão protegendo. Nesse caso, considere mover o servidor de backup primário para uma instância do EC2 para protegê-lo de desastres on-premises e para obter alta disponibilidade.

Para gerenciar os fluxos de dados de backup, você pode criar um ou mais servidores de mídia em instâncias do EC2 na mesma região dos servidores que eles protegerão. Servidores de mídia próximos às instâncias do EC2 economizam dinheiro na transferência pela internet. Quando você faz backup no Amazon S3, os servidores de mídia aumentam o desempenho geral de backup e recuperação.

Você também pode usar o Storage Gateway para fornecer acesso centralizado na nuvem a dados de data centers e escritórios geograficamente dispersos. Por exemplo, um gateway de arquivos oferece acesso sob demanda e de baixa latência aos dados armazenados em AWS fluxos de trabalho de aplicativos que podem abranger todo o mundo. Você pode usar atributos como atualização de cache para atualizar dados em locais distribuídos geograficamente para que o conteúdo possa ser facilmente compartilhado em seus escritórios.


AWS Cloud
Amazon S3 Glacier
Amazon S3
Email notification
Amazon CloudWatch
VPC
Elastic Load Balancing
Active Directory
Jump server
Infrastructure servers
Web servers
Application servers
Databases
Colocation center
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Storage
Firewall and router
Corporate data center
Firewall and router
AWS Storage Gateway
Infrastructure servers
Web servers
Application servers
Databases
Storage
Branch office
Firewall and router
AWS Storage Gateway

# Recuperação de desastres com AWS

As abordagens de backup e restauração e os serviços e tecnologias de suporte podem ser utilizados para implementar sua solução de recuperação de desastres (DR). Muitas empresas estão usando a AWS nuvem para backup e restauração e como um site de DR. AWS fornece vários serviços e recursos que oferecem suporte à recuperação de desastres e à continuidade dos negócios.

Tópicos


- On-premises DR para AWS
- DR para workloads nativos de nuvem

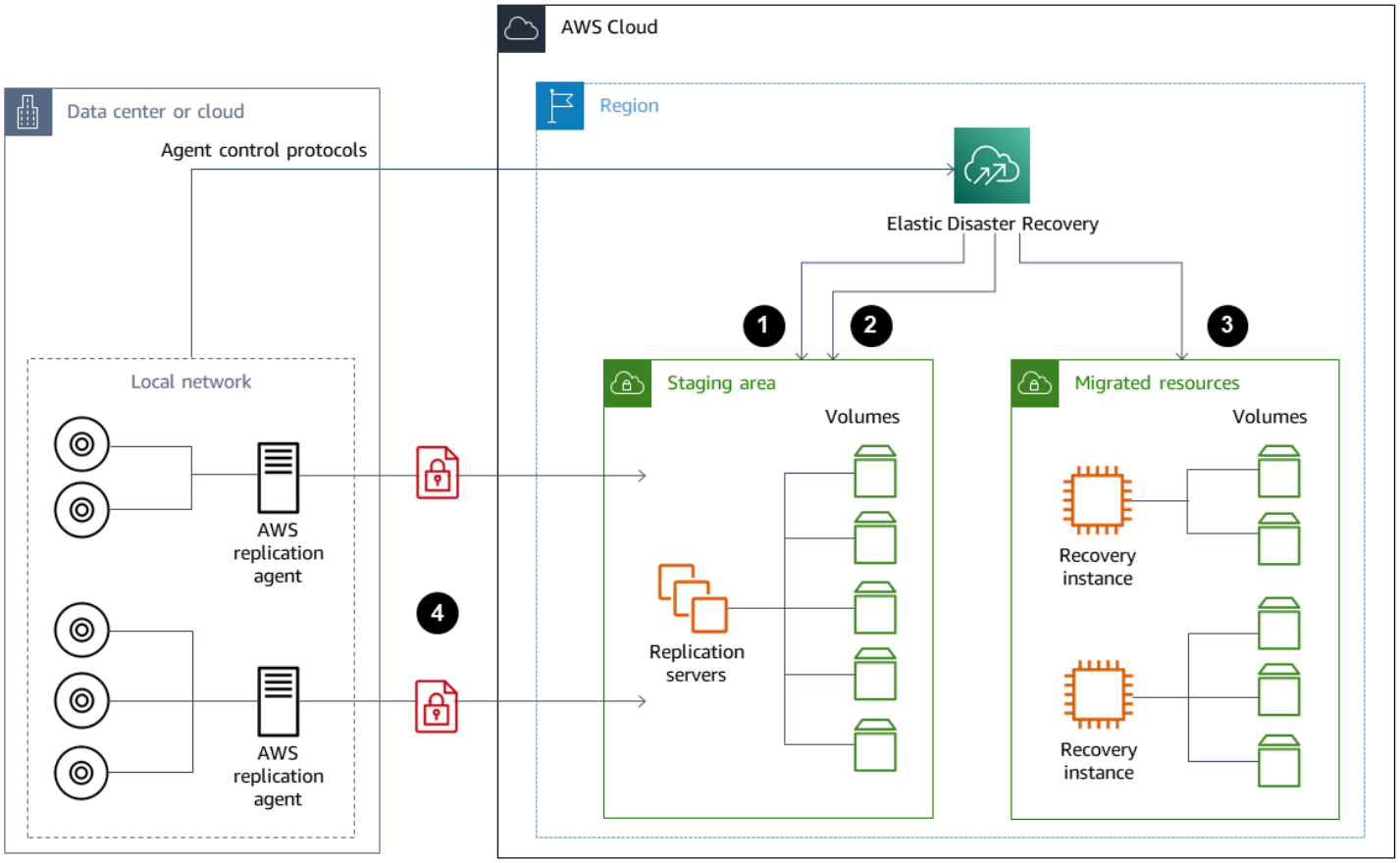

## On-premises DR para AWS

Usar AWS como um ambiente externo de recuperação de desastres (DR) para cargas de trabalho locais é um cenário híbrido comum. Defina seus objetivos de DR, incluindo o tempo de recuperação e os objetivos de ponto de recuperação necessários, antes de selecionar as tecnologias a serem utilizadas. Para ajudar com essa definição, você pode utilizar a lista de verificação do plano de DR.

Há várias opções disponíveis para ajudá-lo a configurar e provisionar rapidamente um ambiente de DR em AWS. Certifique-se de considerar todas as dependências de workload e testar seu plano e sua solução de DR de forma completa e regular para verificar sua integridade.

AWS fornece Recuperação de desastres do AWS Elastica criação de uma réplica completa de seus servidores locais, incluindo o volume raiz e o sistema operacional, em. AWS Recuperação de desastres elástica replica continuamente seus equipamentos em uma área de armazenamento de baixo custo em sua conta AWS alvo e Região da AWS preferida. A replicação em nível de bloco é uma réplica exata do armazenamento de seus servidores, incluindo o sistema operacional, a configuração do estado do sistema, bancos de dados, aplicativos e arquivos. Se houver um desastre, você pode instruir recuperação de desastres elástica para iniciar rapidamente, em minutos, milhares de suas máquinas em seu estado totalmente provisionado.

Recuperação de desastres elástica utiliza um agente instalado em cada um dos seus servidores on-premises. Os atendentes sincronizam o estado de seus servidores on-premises com equivalentes de baixa potência do Amazon EC2 em execução em AWS. Você também pode automatizar seu processo de failover e failback de DR com recuperação de desastres elástica. Automatizar seu processo de failover e failback pode ajudá-lo a alcançar um objetivo de tempo de recuperação (RTO) mais baixo e mais consistente.




1. Relatórios de status do servidor de replicação
2. Recursos da área de preparação criados e encerrados automaticamente
3. Instâncias de recuperação lançadas com RTO de minutos e RPO de segundos
4. Replicação contínua em nível de bloco (compactada e criptografada)

É importante testar o processo de DR e verificar se o ambiente de preparação ao vivo não cria conflitos com o ambiente on-premises. Por exemplo, confirme se as licenças apropriadas estão disponíveis e funcionando em seu ambiente on-premises, de teste e de recuperação de desastres iniciado. Além disso, confirme se todos os processos do tipo processador que possam pesquisar e extrair trabalho de um banco de dados central estão configurados adequadamente para evitar sobreposições ou conflitos. Em seu processo de DR, inclua todas as etapas necessárias que devem ser executadas antes que as instâncias do servidor de recuperação fiquem on-line. Inclua também as etapas a serem executadas depois que as instâncias do servidor de recuperação estiverem on-line e disponíveis. Você pode utilizar soluções como a Solução de automação de planejamento Recuperação de desastres do AWS Elastic ou outra abordagem para ajudá-lo a automatizar seus planos de DR.

Você pode usar um Gateway de volumes do Storage Gateway para fornecer volumes baseados em nuvem a servidores on-premises. Esses volumes também podem ser provisionados rapidamente para uso com o Amazon EC2 usando snapshots do Amazon EBS. Em particular, esses gateways de volumes armazenados oferecem aos aplicativos on-premises acesso de baixa latência aos conjuntos de dados. Os gateways de volume também fornecem backups duráveis baseados em snapshots que podem ser restaurados para uso on-premises ou para uso com o Amazon EC2. Você pode agendar instantâneos pontuais com base no objetivo de ponto de recuperação (RPO) para seu workload.

> **Important**
>
> Os volumes do Gateway de volumes devem ser usados como volumes de dados e não como volumes de inicialização.

Você pode usar uma Imagem de máquina da Amazon (AMI) do Amazon EC2 com uma configuração que corresponda aos seus servidores on-premises e especifique seus volumes de dados separadamente. Depois de configurar e testar a AMI, provisione as instâncias EC2 da AMI junto com os volumes de dados com base nos instantâneos do Gateway de volumes. Essa abordagem exige que você teste seu ambiente minuciosamente para verificar se sua instância do EC2 está operando adequadamente, especialmente para workloads do Windows.

## DR para workloads nativos de nuvem

Considere como suas cargas de trabalho nativas da nuvem se alinham aos seus objetivos de DR. AWS fornece várias zonas de disponibilidade em regiões ao redor do mundo. Muitas empresas que utilizam a nuvem AWS alinham suas arquiteturas de workload e objetivos de DR para suportar a perda de uma zona de disponibilidade. O pilar de confiabilidade na AWS Well-Architected estrutura apóia essa melhor prática. Você pode arquitetar seus workload e suas dependências de serviços e aplicativos para usar várias zonas de disponibilidade. Você pode então automatizar sua DR e atingir seus objetivos de DR com mínima ou nenhuma intervenção.

Na prática, no entanto, você pode descobrir que não consegue estabelecer uma arquitetura redundante, ativa e automatizada para todos os seus componentes. Examine cada camada de sua arquitetura para determinar os processos de DR necessários para atingir seus objetivos. Isso pode variar de workload para workload, com diferentes requisitos de arquitetura e serviço. Este guia aborda as considerações e opções para o Amazon EC2. Para outros serviços AWS , você pode consultar a documentação do AWS para determinar a alta disponibilidade e as opções de DR.

## DR para o Amazon EC2 em uma zona de disponibilidade única

Tente arquitetar seu workload para oferecer suporte e atender ativamente clientes de várias zonas de disponibilidade. Você pode usar o Amazon EC2 Auto Scaling e o Elastic Load Balancing para Multi-AZ obter uma arquitetura de servidor para o Amazon EC2 e outros serviços.

Se sua arquitetura contém instâncias do EC2 que não podem ter balanceamento de carga e podem ter apenas uma única instância em execução a qualquer momento, você pode usar uma das opções a seguir.

- Crie um grupo do Auto Scaling que tenha os tamanhos mínimo, máximo e desejado de 1 e esteja configurado para várias zonas de disponibilidade. Crie uma AMI que possa ser usada para substituir a instância se ela falhar. Certifique-se de definir a automação e a configuração adequadas para que uma instância recém-provisionada da AMI possa ser configurada automaticamente e fornecer serviços. Crie um balanceador de carga que aponte para o grupo do Auto Scaling e esteja configurado para várias zonas de disponibilidade. Opcionalmente, crie um alias do Amazon Route 53 que aponte para o endpoint do balanceador de carga.
- Crie um registro do Route 53 para sua instância ativa e faça com que seus clientes se conectem usando esse registro. Crie um script que crie uma nova AMI da sua instância ativa e use a AMI para provisionar uma nova instância do EC2 no estado interrompido em uma zona de disponibilidade separada. Configure o script para ser executado periodicamente e encerrar a instância interrompida anterior. Se houver uma falha na zona de disponibilidade, inicie sua instância de backup na zona de disponibilidade alternativa. Em seguida, atualize o registro do Route 53 para apontar para essa nova instância.

Teste sua solução minuciosamente simulando a falha contra a qual a solução foi projetada para proteger. Considere também as atualizações que sua solução de DR precisará à medida que sua arquitetura de workload mudar.

## DR para Amazon EC2 em uma falha regional

Clientes com requisitos de disponibilidade muito altos (por exemplo, aplicativos de missão crítica que não toleram nenhum tempo de inatividade) podem usar AWS em várias regiões para fornecer maior resiliência contra problemas em nível regional. Os clientes devem avaliar cuidadosamente a complexidade, o custo e o esforço necessários para estabelecer e manter um plano de DR multirregional em relação ao benefício. AWS fornece recursos que oferecem suporte a arquiteturas

multirregionais para disponibilidade global, failover e DR. Este guia aborda alguns dos recursos disponíveis que são específicos para backup e recuperação do Amazon EC2.

AWS As AMIs e os snapshots do Amazon EBS são recursos regionais que podem ser usados para provisionar novas instâncias em uma única região. No entanto, você pode copiar seus snapshots e AMIs para outra região e utilizá-los para provisionar novas instâncias nessa região. Para dar suporte a um plano regional de recuperação de desastres para falhas, você pode automatizar o processo de cópia de AMIs e snapshots para outras regiões. AWS Backup e o Amazon Data Lifecycle Manager oferecem suporte à cópia entre regiões como parte de sua configuração de backup.

Recuperação de desastres do AWS Elastic pode ser usado para automatizar e replicar continuamente seus servidores Amazon EC2 em uma região para uma região alternativa de DR. A recuperação de desastres elástica pode simplificar sua abordagem de DR em várias regiões e ajudá-lo a testar regularmente seu plano de DR entre regiões do Amazon EC2 usando simulações. A recuperação de desastres elástica pode ajudar quando o backup e a recuperação não conseguirem atingir seus objetivos de RTO e RPO. A recuperação de desastres elástica pode ajudá-lo a reduzir seu RTO para minutos e seu RPO para uma faixa de menos de um segundo.

Qualquer que seja a solução utilizada, você deve determinar o processo de provisionamento, failover e failback a ser usado no caso de uma interrupção. Você pode utilizar o Route 53 com verificação de integridade e failover do Sistema de Nomes de Domínio para ajudar a oferecer suporte à sua solução.

# Limpeza dos backups

Para reduzir custos, limpe os backups que não são mais necessários para fins de recuperação ou retenção. Você pode usar o AWS Backup Amazon Data Lifecycle Manager para automatizar sua política de retenção para uma parte dos seus backups. No entanto, mesmo com essas ferramentas instaladas, você ainda precisa de uma abordagem de limpeza para backups feitos separadamente.

Uma estratégia de marcação é um pré-requisito para uma estratégia de limpeza. Use a marcação para identificar os recursos que devem ser limpos, notifique os proprietários adequadamente e automatize seu processo de limpeza. Os backups criados por AWS têm datas de criação alinhadas a eles, mas a marcação é importante para correlacionar os backups às suas cargas de trabalho, aos requisitos de retenção e à identificação do ponto de restauração.

Você pode implementar um processo de limpeza para instantâneos usando a automação. Por exemplo, você pode escanear sua conta em busca de instantâneos e determinar se os volumes correspondentes estão em um estado anexado ou disponível. Você pode filtrar ainda mais os resultados em um limite de tempo especificado. Usando as tags anexadas ao volume, você pode enviar e-mails automaticamente aos proprietários dos instantâneos e avisá-los de que seus instantâneos foram programados para exclusão. Essa remediação automatizada pode ser implementada usando AWS Config regras, um script usando o AWS CLI ou uma função Lambda usando AWS o SDK.

O Systems Manager fornece os DeleteSnapshot documentos AWS-Delete EBSVolume Snapshots e AWS- para ajudá-lo a iniciar e automatizar a limpeza dos snapshots do Amazon EBS. Você também pode usar o AWS SDK AWS CLI e para automatizar a limpeza de outros AWS recursos, como snapshots do Amazon RDS.

# Perguntas frequentes sobre backup e recuperação

## Qual cronograma de backup devo selecionar?

Defina uma frequência de cronograma de backup que esteja alinhada ao seu objetivo de ponto de recuperação (RPO). Defina um horário de backup quando seu workload estiver sob a menor quantidade de carga e quando o impacto ao usuário puder ser reduzido. Crie um point-in-time instantâneo sempre que você fizer uma alteração significativa em sua carga de trabalho.

## Preciso criar backups em minhas contas de desenvolvimento?

Teste alterações potencialmente significativas em suas contas de desenvolvimento para seus workloads e crie backups antes de realizar alterações significativas. Você pode ter muitos outros backups de point-in-time recuperação (PITR) em suas contas de desenvolvimento e de não produção das atividades de desenvolvimento e teste.

## Posso atualizar aplicativos e continuar usando um volume do EBS enquanto um snapshot estiver sendo criado sem qualquer impacto?

Os snapshots ocorrem de forma assíncrona; o point-in-time snapshot é criado imediatamente, mas o status do snapshot fica pendente até que todos os blocos modificados tenham sido transferidos para o Amazon S3. Para snapshots iniciais grandes ou subsequentes em que muitos blocos forem alterados, a transferência pode levar várias horas. Enquanto está sendo transferido, um snapshot em andamento não é afetado pelas leituras e gravações contínuas do volume. Para obter mais informações, consulte a documentação do AWS.

# Próximas etapas

Comece avaliando, implementando e testando sua abordagem de backup e recuperação em um ambiente que não seja de produção. É importante testar minuciosamente o processo de recuperação e validar se os workloads restaurados estão operando conforme o esperado.

Teste o processo de restauração de um único componente em sua arquitetura, além de todos os componentes em sua arquitetura. Valide o tempo de recuperação de cada um. Além disso, valide o impacto do seu processo de backup e restauração nas dependências a upstream e downstream. Confirme o impacto de qualquer interrupção do serviço em suas dependências upstream e confirme o impacto downstream em seus backups.

# Recursos adicionais do

## AWS recursos

- AWS Orientação prescritiva
- AWS documentação
- AWS referência geral
- Glossário da AWS

## AWS serviços

- AWS Backup
- Amazon CloudWatch
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- Amazon EventBridge
- IAM
- Amazon RDS
- Amazon S3
- Storage Gateway
- AWS Systems Manager

## Outros recursos

- Backup e recuperação com AWS Backup (solução)
- Recuperação de cargas de trabalho em desastres em AWS: Recuperação na nuvem (white paper)
- Série de recuperação de desastres (publicações do blog sobre AWS arquitetura)
- Lista de verificação do plano de recuperação de desastres de TI
- Abordagens de backup e recuperação utilizando AWS (publicação técnica — arquivadas)
- Começando com AWS Backup

# Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Informações atualizadas | Orientação atualizada na seção sobre o Amazon S3. | 28 de junho de 2024 |
| Informações atualizadas | Informações atualizadas na seção DR On-premises para AWS. | 13 de abril de 2023 |
| Uma seção adicionada | Foram adicionadas orientaçõ es e etapas para criar ou restaurar uma instância a partir de um snapshot. | 7 de março de 2023 |
| Informações foram adicionad as sobre recuperação de desastres elástica e esclareci mentos adicionais | Nas seções Recuperação de desastres com AWS e Escolha de AWS serviços para proteção de dados, foram adicionadas informaçõ es sobre Recuperação de desastres do AWS Elastic. Nas seções EC2 Backup e recuperação da Amazon com snapshots e AMIs, Preparand o um volume do EBS antes de criar um snapshot ou AMI e Restauração a partir de um snapshot do Amazon EBS ou de uma AMI, acrescentei esclarecimentos. Adicionado às Perguntas frequentes sobre backup e recuperação. | 19 de janeiro de 2023 |

| | | |
|---|---|---|
| Um link foi adicionado | Foi adicionado um link para a documentação do Amazon Data Lifecycle Manager na seção Amazon Data Lifecycle Manager. | 31 de outubro de 2022 |
| Informações atualizadas | As informações sobre a restauração de volumes foram atualizadas. | 30 de agosto de 2022 |
| Informações atualizadas e nova seção adicionada | Na seção Escolha AWS de serviços para proteção de dados, serviços adicionados. Foi adicionada a seção Backup e recuperação usando AWS Backup. Na seção Backup e recuperação usando o Amazon S3 e o Amazon Glacier, informações foram adicionadas sobre as novas classes de armazenamento do Amazon Glacier. Na seção Backup e recuperação para Amazon EC2 com volumes do EBS, foram adicionados links para documentação e informações adicionais. Na seção Backup e recuperação de AWS serviços nativos em nuvem, adicionei uma recomendação de uso. AWS Backup Na seção Recursos adicionais, recursos foram adicionados. | 28 de janeiro de 2022 |

| | | |
|---|---|---|
| Informações atualizadas | Foram adicionadas informaçõ es sobre a configuração de classes de armazenam ento à seção Recuperaç ão Flexível do S3 Glacier. Foram adicionadas informaçõ es sobre a recuperação de snapshots para o EC2 backup e recuperação da Amazon com snapshots e seção. AMIs | 9 de setembro de 2021 |
| Informações atualizadas | Na AWS Backupseção, foram adicionadas informaçõ es sobre os AWS serviços que oferecem AWS Backup suporte. | 1º de junho de 2021 |
| Publicação inicial | — | 29 de julho de 2020 |

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.