Abordagens de backup e recuperação em AWS

AWS Orientação prescritiva

AWS Orientação prescritiva: Abordagens de backup e recuperação em AWS

Table of Contents

Abordagens de backup e recuperação na AWS

Khurram Nizami, Amazon Web Services (AWS)

Abril de 2023 (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 utilizados para criar soluções de proteção de dados escaláveis e confiáveis para os componentes não imutáveis da sua arquitetura.

Outra abordagem é modernizar seus workloads para utilizar 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:

- Tecnologia sem servidor com AWS Lambda
- Contêiner com Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) e AWS Fargate
- Imagem de máquina da Amazon (AMI) 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:

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

Por que utilizar AWS como plataforma de proteção de dados?

A AWS é uma plataforma de computação em nuvem segura, de alto desempenho, flexível, econômica e fácil de usar. 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 da sua estratégia de proteção de dados:

- Durabilidade: o Amazon Simple Storage Service (Amazon S3), o Amazon S3 Glacier 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 serviços AWS utilizam o Amazon S3 para operações de armazenamento e exportação/importação. 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 serviços AWS 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 workload.
- Conformidade: a infraestrutura AWS 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 operações AWS reduz os custos do serviço e ajuda a reduzir o TCO dos serviços AWS. AWS repassa essa economia de custos aos clientes por meio de quedas de preços.
- Preço conforme o uso: adquira serviços AWS conforme necessário e somente pelo período em que planeja utilizá-los. O preço do AWS 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 serviços AWS que você pode utilizar para oferecer suporte às abordagens de backup e recuperação para o seguinte:

- Arquitetura on-premises
- Arquiteturas nativas de nuvem
- Arquiteturas híbridas
- Serviços nativos da AWS
- 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

> **Aviso**
>
> Em 30 de abril de 2024, o VMware Cloud on não AWS é mais revendido AWS nem por seus parceiros de canal. O serviço continuará disponível pela Broadcom. Recomendamos que você entre em contato com seu AWS representante para obter detalhes.

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 e o Amazon S3 Glacier e o S3 Glacier Deep Archive são adequados para casos de uso híbridos e nativos de nuvem. Esses serviços fornecem soluções de armazenamento de objetos altamente duráveis e de uso geral, adequadas para fazer backup de arquivos individuais, servidores ou de um datacenter 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
  - Amazon S3 Glacier
  - 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
  - Cargas de trabalho da VMware no local e no VMware Cloud on AWS
  - 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.
- AWS Elastic Disaster Recoveryreplica continuamente suas máquinas em uma área de armazenamento de baixo custo em sua AWS conta-alvo e região preferida. Você pode usar o Elastic Disaster Recovery para premises-to-cloud DR e 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 o Amazon CloudWatch Events 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 e Amazon S3 Glacier

O Amazon S3 e o Amazon S3 Glacier são serviços de armazenamento ideais para uso em arquiteturas on-premises, híbridas e nativas de nuvem. Esses serviços fornecem plataformas de armazenamento duráveis e de baixo custo que oferecem capacidade escalável e não exigem gerenciamento de volume ou mídias à medida que seus conjuntos de dados de backup crescem. O modelo pay-for-what-you -use e o baixo custo por GB/mês tornam esses serviços adequados para uma ampla variedade de casos de uso de proteção de dados.

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

Tópicos

Amazon S3

Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume 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 os SDKs AWS CLI ou.

AWS os serviços usam 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.

O Amazon S3 oferece uma variedade de classes de armazenamento para diferentes casos de uso, incluindo os casos a seguir:

- S3 Standard para armazenamento de uso geral de dados acessados com frequência (por exemplo, arquivos de configuração, backups não planejados, backups diários).
- S3 Standard-IA para dados de longa duração, mas acessados com menos frequência (por exemplo, backups mensais). IA (Infrequent Access) é a sigla em inglês para acesso pouco frequente.

O Amazon S3 também oferece políticas de ciclo de vida configuráveis para gerenciar seus dados durante o ciclo de vida. Assim que uma política é definida, seus dados migram automaticamente para a classe de armazenamento apropriada sem nenhuma alteração no seu aplicativo. 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

Você pode automatizar a transição de seus backups usando o gerenciamento do ciclo de vida de objetos.

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

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 os AWS CLI AWS SDKs e as operações de API 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 o 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.

Amazon S3 Glacier

O Amazon S3 Glacier é um serviço de armazenamento de arquivos em nuvem de baixo custo que fornece armazenamento seguro e durável para arquivamento de dados e backup online. Para manter os custos baixos, o S3 Glacier fornece três classes de armazenamento, de alguns milissegundos a horas. O S3 Glacier Flexible Retrieval e o S3 Glacier Deep Archive oferecem opções adicionais com base na rapidez com que você precisa restaurar os dados. Com o S3 Glacier, você pode armazenar

de forma confiável grandes ou pequenas quantidades de dados com economias significativas em comparação com as soluções on-premises. O S3 Glacier é bem adequado para armazenamento de dados de backup com requisitos de retenção longos ou indefinidos e para arquivamento de dados de longo prazo. O S3 Glacier fornece as seguintes classes de armazenamento:

- S3 Glacier Instant Retrieval para arquivar dados que podem ser necessários uma vez por trimestre e precisam ser restaurados rapidamente (milissegundos)
- S3 Glacier Flexible Retrieval para arquivar dados que talvez precisem ser restaurados uma ou duas vezes por ano, em poucas horas
- S3 Glacier Deep Archive para arquivar dados do ciclo de backup de longo prazo que talvez precisem ser restaurados com pouca frequência dentro de 12 horas

A tabela a seguir resume as opções de recuperação de arquivos.

Classe de armazenamento	Expressa	Padrão	Em massa
S3 Glacier Instant Retrieval	Não aplicável	Não aplicável	Não aplicável
S3 Glacier Flexible Retrieval	1 a 5 minutos	3 a 5 horas	5 a 12 horas
S3 Glacier Deep Archive	Não disponível	Em 12 horas	Em 48 horas

Usando o Amazon S3, você pode definir a classe de armazenamento para cada objeto em seu bucket do S3 ao criá-lo. Depois que o objeto é criado, você pode alterar a classe de armazenamento copiando o objeto para um novo objeto com uma classe de armazenamento diferente. Ou você pode ativar uma configuração de ciclo de vida que irá alterar automaticamente a classe de armazenamento dos objetos com base nas regras que você especificar.

Para automatizar seus processos de backup e restauração, você pode acessar o Amazon S3 Glacier e o S3 Glacier Deep Archive por meio dos SDKs, e. AWS Management Console AWS CLI AWS Para obter mais informações, consulte Amazon S3 Glacier.

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

Usando a transição de objetos do Amazon S3 Lifecycle para o Amazon S3 Glacier em comparação com o gerenciamento de arquivos do Amazon S3 Glacier

O Amazon S3 fornece uma transição conveniente de objetos do S3 para as classes de armazenamento do Amazon S3 Glacier para que você possa gerenciar o ciclo de vida e os custos dos seus backups. No entanto, dependendo do tamanho dos objetos e da sua necessidade de restaurar uma coleção de objetos para diferentes componentes na sua arquitetura, talvez você queira gerenciar esse processo por conta própria.

Se você tiver um grande número de objetos pequenos que precisem ser restaurados coletivamente, considere as implicações de custo das seguintes opções:

- Usando uma política de ciclo de vida para fazer a transição automática de objetos individualmente para o Amazon S3 Glacier
- Compactando objetos em um único arquivo e armazenando-os no Amazon S3 Glacier

O Amazon S3 Glacier tem tarifas mínimas de capacidade para cada objeto, dependendo da classe de armazenamento que você usa. Por exemplo, o S3 Glacier Instant Retrieval tem uma tarifa de capacidade de 128 KB para cada objeto. Consulte o gráfico de desempenho para up-to-date obter mais informações.

Para cada objeto arquivado no S3 Glacier Flexible Retrieval ou no S3 Glacier Deep Archive, o Amazon S3 usa 8 KB de armazenamento para o nome do objeto e outros metadados. O Amazon S3 armazena esses metadados de modo que você possa obter uma lista em tempo real de seus objetos arquivados usando a API do Amazon S3. Você é cobrado com as tarifas S3 Standard pelo armazenamento adicional.

O Amazon S3 também adiciona 32 KB de armazenamento por indexação e metadados relacionados para cada objeto arquivado nas categorias de armazenamento S3 Glacier Flexible Retrieval ou

S3 Glacier Deep Archive. Esses dados adicionais são necessários para identificar e recuperar seu objeto. As tarifas do Amazon S3 Glacier ou S3 Glacier Deep Archive são cobradas de você por esse armazenamento adicional.

Ao compactar seus objetos em um único arquivo, você pode reduzir o armazenamento adicional usado pelo Amazon S3 Glacier, bem como evitar cobranças mínimas de capacidade para muitos objetos pequenos.

Outra consideração importante é que as políticas de ciclo de vida são aplicadas aos objetos individualmente. Isso pode afetar a integridade do seu backup se uma coleção de objetos precisar ser restaurada coletivamente a partir de uma data específica. Não há garantia de que todos os objetos façam a transição ao mesmo tempo, ainda que tiverem o mesmo tempo de expiração e ciclo de vida de transição definidos entre os objetos. Pode haver um atraso entre quando a regra do ciclo de vida é satisfeita e quando ação para tal regra é concluída. Para mais informações, consulte o Centro de Conhecimentos da AWS.

Por fim, considere o esforço de restauração entre o uso de arquivos de políticas de ciclo de vida e o gerenciamento de um arquivo separado criado por você. Você deve iniciar uma restauração para cada objeto do Amazon S3 Glacier separadamente. Isso exige que você crie um script ou use uma ferramenta para iniciar a restauração de vários objetos coletivamente. Você pode usar o S3 Batch Operations para ajudar você a reduzir o número de solicitações individuais, ou usar o console do Amazon S3.

Proteger dados de backup no Amazon S3 e no Amazon S3 Glacier

A segurança dos dados é uma preocupação universal e AWS leva a segurança muito a sério. A segurança é a base de cada AWS serviço. Serviços de armazenamento, como o Amazon S3, oferecem recursos sólidos para o controle de acesso e criptografia, tanto em repouso quanto em trânsito. Todos os endpoints de API do Amazon S3 e do Amazon S3 Glacier oferecem suporte a Secure Sockets Layer/Transport Layer Security (SSL/TLS) para criptografar dados em trânsito. O Amazon S3 Glacier criptografa todos os dados em repouso por padrão. Com o Amazon S3, você pode escolher a criptografia feita pelo servidor para objetos em repouso fazendo o seguinte:

- Como usar criptografia feita pelo servidor com chaves de criptografia gerenciadas pelo Amazon S3
- Usando criptografia do lado do servidor com chaves AWS Key Management Service (AWS KMS) armazenadas em AWS KMS

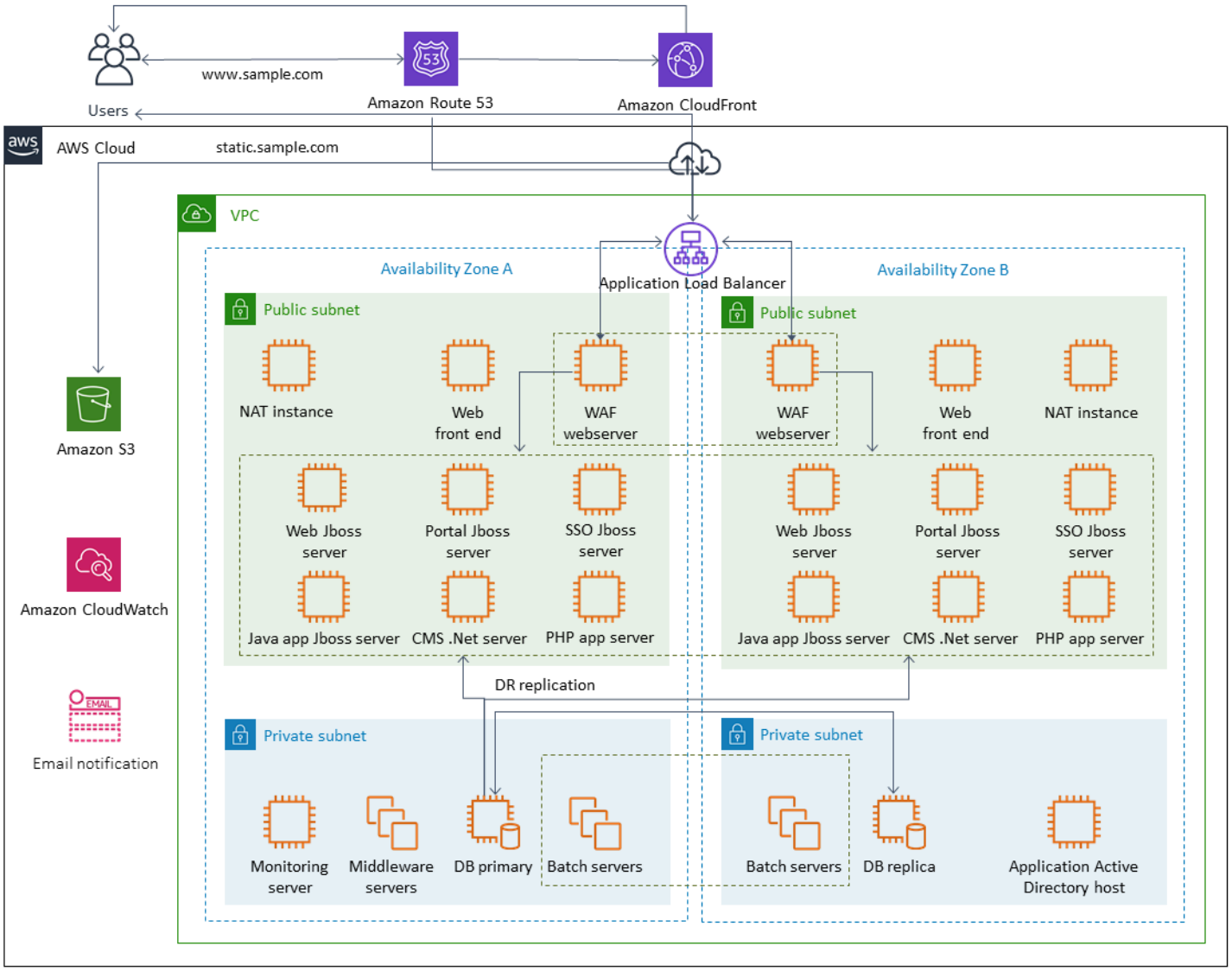
Como alternativa, você pode criptografar seus dados antes de enviá-los para o. AWS Para obter mais informações, consulte a documentação sobre criptografia do lado do cliente.

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 os logs no nível de objetos 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 aplicativos, servidores de monitoramento, bancos de dados e Active Directory.



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

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 snapshots. As nstance-store-backed 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.

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 EC2 em execução no Linux ou no Windows. Quando quiser reverter, use o assistente de inicialização da instância para criar uma instância. No assistente de execução da instância, escolha Minhas AMIs.
- Para fazer backup de um volume individual, crie um instantâneo. Para restaurar o instantâneo, consulte Criar um volume a partir de um instantâneo. Você pode usar o AWS Management Console 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 dos metadados. O custo de um snapshot do EBS é o armazenamento do volume individual. Para obter mais informações sobre 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 recurso de snapshot para fazer point-in-time backups 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 EC2 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 EC2. 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 Centro de Conhecimentos da AWS.

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 manter o sistema em um estado em que não esteja executando qualquer E/S. O ideal é que o equipamento não esteja aceitando tráfego e esteja parado, mas isso é raro, pois operações de TI 24 horas por dia, 7 dias por semana, 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 poderá facilitar esse processo utilizando um gerenciador de volume lógico que ofereça suporte ao congelamento de E/S.

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 em nível de imagem de aplicativos compatíveis com VSS. 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.

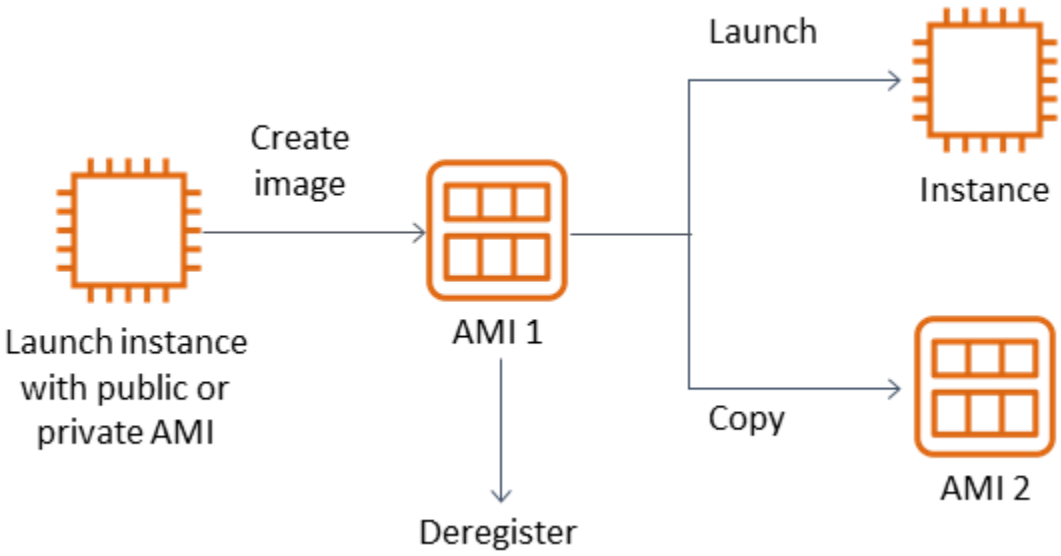
Insira uma descrição e adicione as tags apropriadas. Adicione uma tag `Name` para facilitar a localização do volume posteriormente. Adicione outras tags apropriadas com base na sua estratégia de marcação.

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

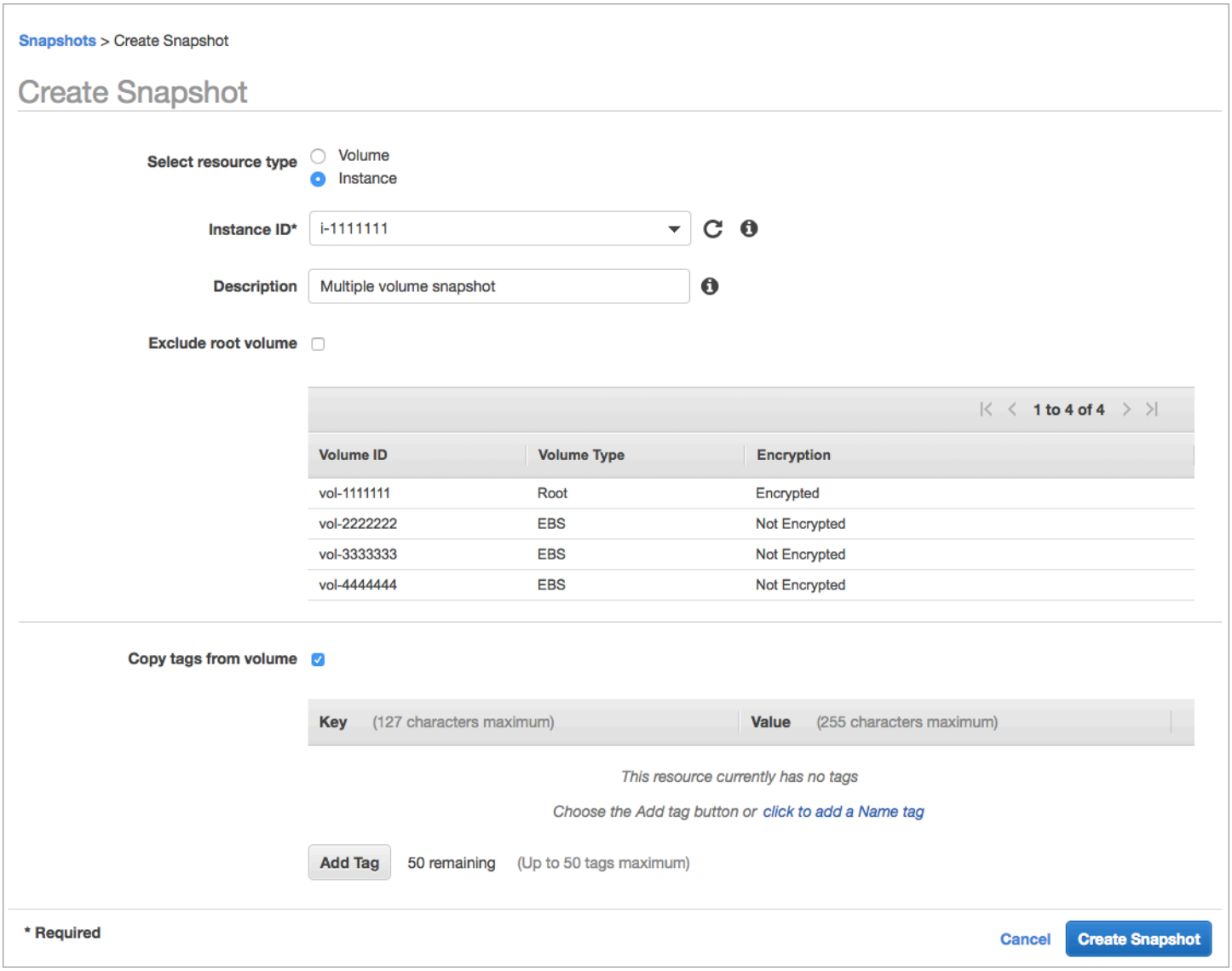
AWS Backup é exclusivo do Amazon Data Lifecycle Manager porque você pode criar um plano de backup que inclui recursos em vários serviços. AWS Você poderá coordenar seu backup para cobrir os recursos que você estiver usando juntos, em vez de coordenar os backups dos recursos individualmente.

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 snapshots de instâncias que possuem vários volumes conectados em uma configuração RAID são obtidos como snapshots de vários volumes, coletivamente. Os instantâneos de vários volumes fornecem point-in-time instantâneos coordenados com dados e consistentes em falhas em vários volumes do EBS conectados a uma instância do EC2. Não é necessário interromper a instância para coordenar entre volumes a fim de 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 da 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 contas da AWS, poderá designar uma conta separada como sua conta de arquivamento para a qual todas as outras contas podem 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 consiga reproduzir instâncias do EC2 em outra região da AWS em caso de 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). O 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 EC2 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 end-of-lifecycle etapa para volumes do EBS que não são mais usados. 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 AWS CLI, o e os SDKs AWS

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 CreateImage runbooks da AWS CreateSnapshot e da AWS para criar snapshots e AMIs, ou você pode conceder permissões a outros usuários para usá-los. O Systems Manager também inclui os UpdateWindowsAmi runbooks da AWS UpdateLinuxAmi e da AWS 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 point-in-time exata do volume original que foi 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 AWS CLI, o 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 point-in-time backup 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.

No entanto, 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.

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 on-premises para AWS

Você pode usar a AWS para armazenamento externo durável de seus backups de infraestrutura on-premises. Ao usar serviços de armazenamento da AWS 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 e o Amazon S3 Glacier fornecem operações abrangentes de API e SDKs para integrar esses serviços às suas abordagens novas e existentes de backup e recuperação. Isso também oferece aos fornecedores de software de backup formas de integrar diretamente seus aplicativos às soluções de armazenamento da AWS.

Nesse cenário, o software de backup e arquivamento que você está usando em sua infraestrutura on-premises interage diretamente com a AWS por meio das operações de API. Como o software de backup reconhece a AWS, ele faz backup dos dados dos servidores on-premises diretamente no Amazon S3 ou no Amazon S3 Glacier.

Se seu software de backup existente não oferecer suporte nativo à AWS Cloud, 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 ou no Amazon S3 Glacier. 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 acesso baseado em SMB ou NFS.

- 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 e ao Amazon S3 Glacier. 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

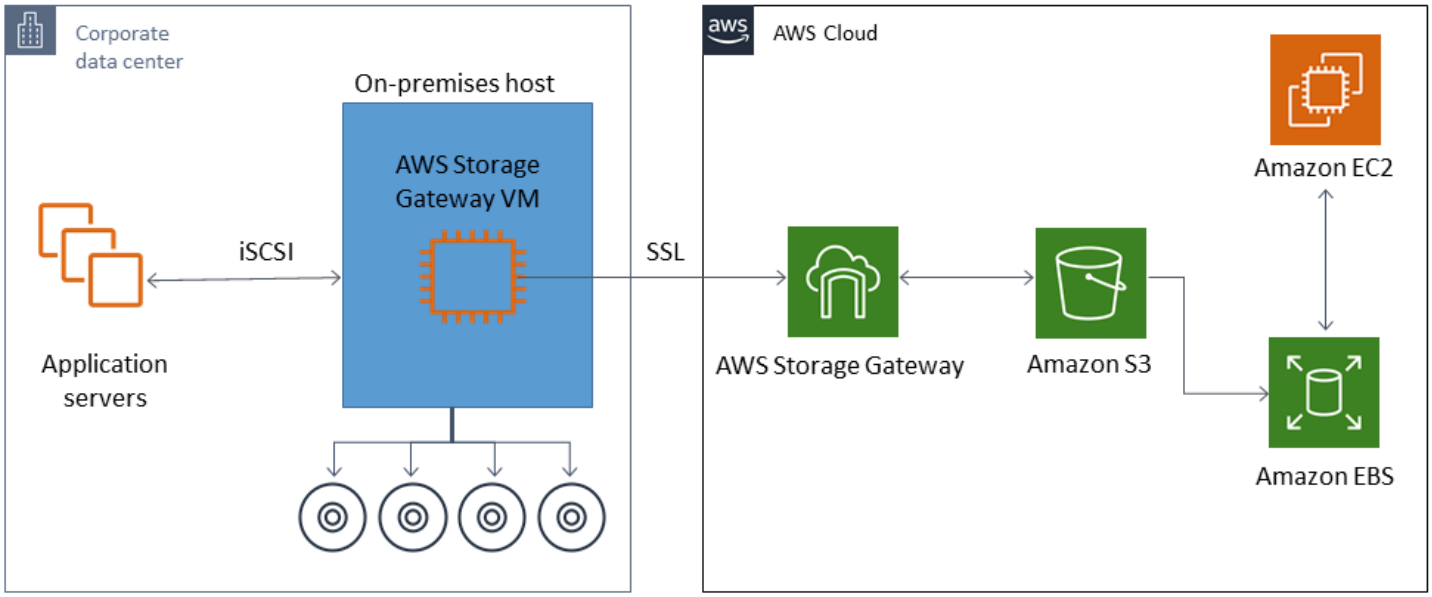
Muitas organizações iniciam sua jornada para a nuvem transferindo dados secundários e terciários, como backups, para a nuvem. O suporte à interface SMB e NFS de um gateway de arquivos fornece uma maneira de os grupos de TI fazerem a transição das tarefas de backup dos sistemas de backup on-premises existentes 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. As necessidades de retenção de longo prazo são atendidas por meio da hierarquização dos backups em níveis de armazenamento de baixo custo do S3 Standard-Infrequent Access e do Amazon S3 Glacier.

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 volumes se integra ao atributo de volume do Amazon EBS do Amazon EC2, você pode usar o AWS Backup 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.

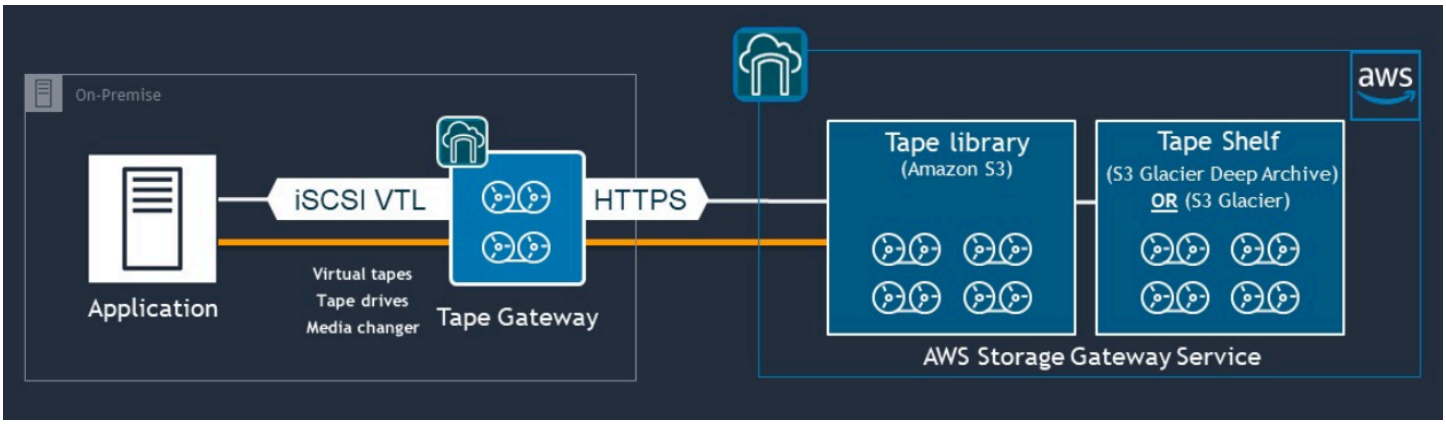
Gateway de fitas

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

A 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 fitas apresenta o Storage Gateway ao seu aplicativo de backup existente como uma VTL baseada em iSCSI de padrão aberto, 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 de biblioteca de fitas baseada em iSCSI 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 do 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 AWS por meio de uma conexão VPN ou por meio de 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 o 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 os SDKs AWS CLI 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 AWS nativos em nuvem

Sua abordagem de backup e recuperação deve abranger os serviços do AWS usados em suas cargas de trabalho. O AWS fornece recursos e opções específicos do serviço para gerenciar e interagir com seus dados. Você pode usar o console, o AWS CLI, os SDKs e as operações de API para implementar o backup e a recuperação dos serviços do AWS 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 oferecem recuperação point-in-time (PITR) de sua instância de BD. Backup automatizado é ativado por padrão quando você cria uma instância de banco de dados.

  O Amazon RDS realiza um backup diário completo 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 no AWS Backup, que também fornece outros recursos. Considere usar o AWS Backup para configurar um plano de backup padrão para seus bancos de dados do 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 AWS CLI, ou a API do DynamoDB. Para obter mais informações, consulte Como fazer backup de uma tabela do DynamoDB. Você pode programar backups periódicos ou futuros usando o AWS Backup, ou você pode personalizar e automatizar sua abordagem de backup usando funções do 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. Caso não queira criar scripts de programação e trabalhos de limpeza, você poderá usar o AWS Backup para criar planos de backup. Os planos de backup incluem agendas e políticas de retenção para suas tabelas do DynamoDB. O AWS Backup cria os backups e exclui os backups anteriores com base no seu cronograma de retenção. O 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
- Métricas e alarmes do Amazon CloudWatch
- 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

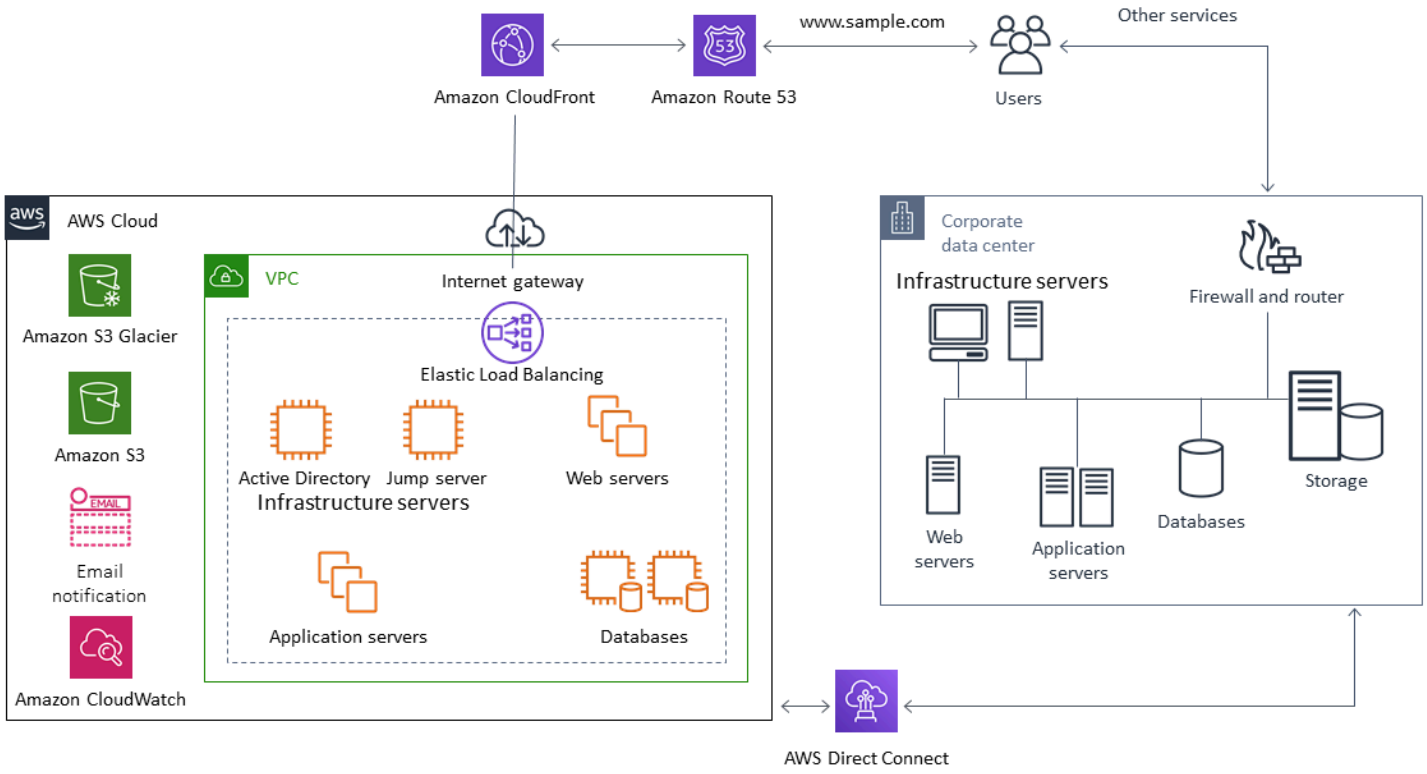
tabela do DynamoDB de um arquivo de configuração, valor do AWS Systems Manager Parameter Store ou outra referência que possa ser atualizada dinamicamente para refletir o nome da tabela que o cliente deve usar.

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 on-premises e nativas de nuvem discutidas neste guia podem ser combinadas em cenários híbridos em que o ambiente de workload tem componentes on-premises e de infraestrutura da AWS. Os recursos, incluindo servidores web, servidores de aplicativos, servidores de monitoramento, bancos de dados e o Microsoft Active Directory, são hospedados no datacenter do cliente ou na AWS. Os aplicativos que estão sendo executados na AWS Cloud são conectados aos aplicativos que estão sendo executados on-premises.

Isso está se tornando um cenário comum para workloads corporativas. Muitas empresas têm datacenters próprios e os usam a AWS para aumentar a capacidade. Esses datacenters de clientes geralmente são conectados à rede da AWS por links de rede de alta capacidade. Por exemplo, com AWS Direct Connect, você pode estabelecer conectividade privada e dedicada do seu datacenter on-premises para a 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.



Soluções de proteção de dados bem projetadas geralmente usam uma combinação das opções descritas nas soluções nativas de nuvem e on-premises neste guia. Muitos ISVs fornecem soluções

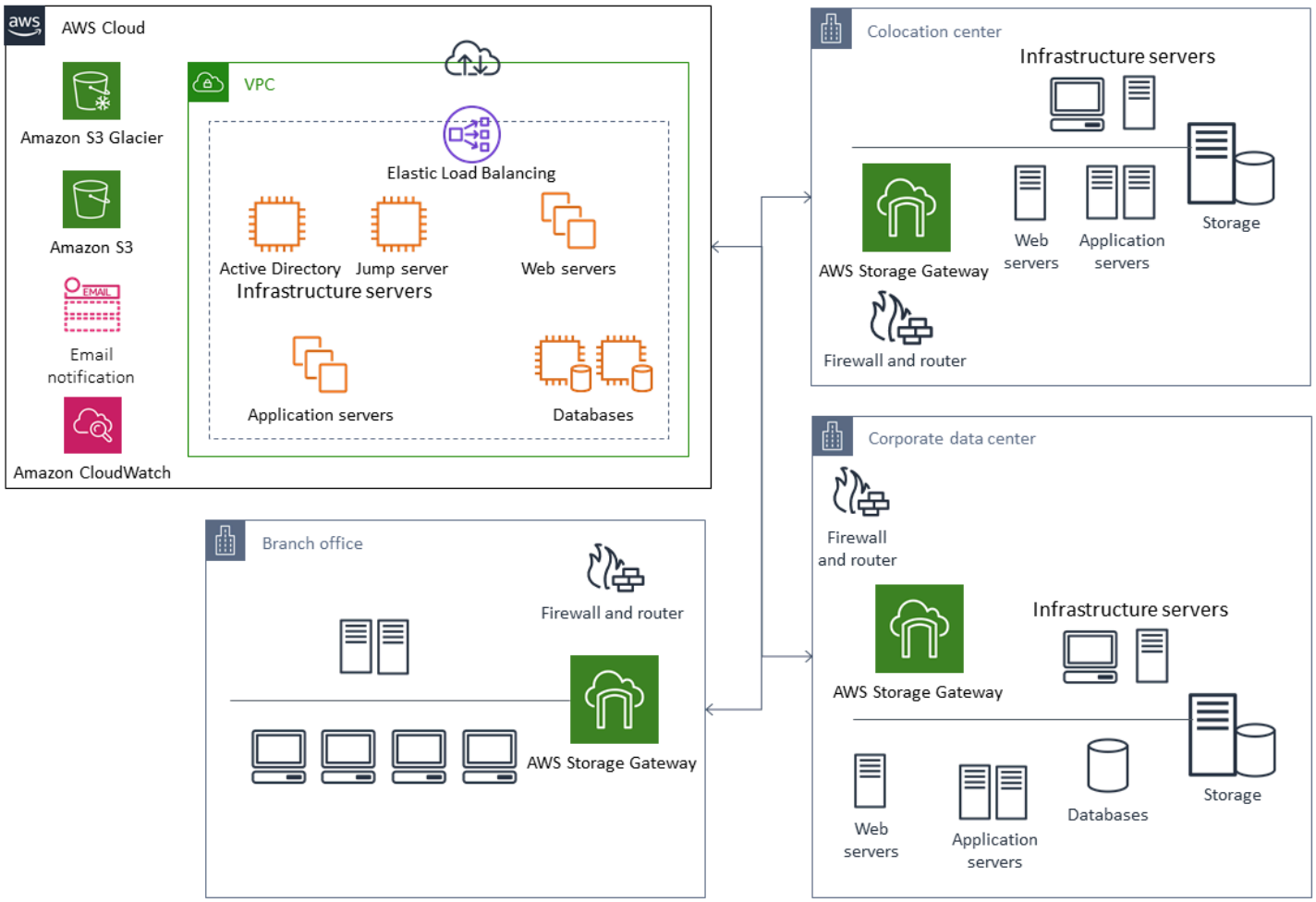
de backup e restauração líderes de mercado para infraestrutura on-premises e expandiram suas soluções para oferecer suporte a abordagens híbridas.

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 a 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 ou no Amazon S3 Glacier, 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 datacenters e escritórios geograficamente dispersos. Por exemplo, um gateway de arquivos oferece acesso sob demanda e de baixa latência aos dados armazenados na AWS para 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
Web servers
Infrastructure 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

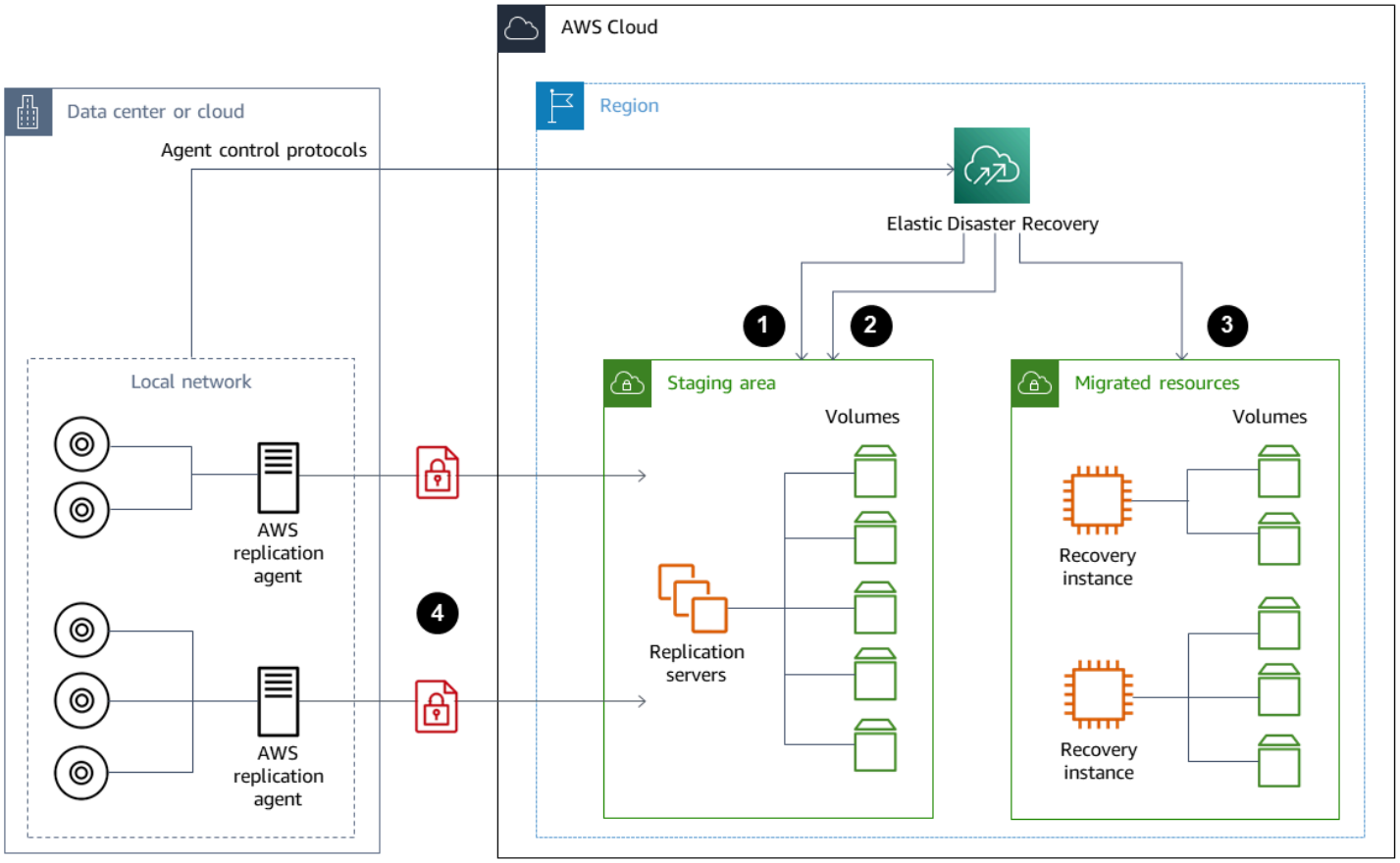
DR local para AWS

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 AWS Elastic Disaster Recoverya 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 AWS Elastic Disaster Recovery 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 programar point-in-time instantâneos com base no objetivo de ponto de recuperação (RPO) para sua carga de trabalho.

> **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 no AWS Well-Architected Framework 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 AWS documentação 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 utilizar o Amazon EC2 Auto Scaling e o balanceador de carga elástica para obter uma arquitetura de servidor Multi-AZ 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.

AWS Elastic Disaster Recovery 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 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 pelo AWS têm datas de criação alinhadas a eles, mas a marcação é importante para correlacionar os backups a 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 regras do AWS Config, um script usando o AWS CLI ou uma função do Lambda usando o SDK AWS.

O Systems Manager fornece os documentos AWS-DeleteEBSVolumeSnapshots e AWS-DeleteSnapshot para ajudá-lo a iniciar e automatizar a limpeza dos snapshots do Amazon EBS. Você também pode usar o SDK AWS CLI e AWS e para automatizar a limpeza de outros recursos do AWS, como os instantâneos 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 snapshot pontual sempre que você fizer uma alteração significativa em seu workload.

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 recuperação para um ponto no tempo (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?

Snapshots ocorrem de forma assíncrona; o snapshot de ponto no tempo é criado imediatamente, mas o status do snapshot ficará pendente até que todos os blocos modificados tenham sido transferidos para 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

Recursos da AWS

- Recomendações da AWS
- Documentação da AWS
- Referência geral da AWS
- Glossário da AWS

Serviços da AWS

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

Outros recursos

- Backup e recuperação com AWS Backup (solução)
- Recuperação de desastres de workloads na AWS: recuperação na nuvem (publicação técnica)
- Série de recuperação de desastres (publicações no blog da AWS Architecture)
- Lista de verificação do plano de DR
- Abordagens de backup e recuperação utilizando AWS (publicação técnica — arquivadas)

- Conceitos básicos do AWS Backup
- AWS Marketplace — Backup e restauração

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	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 Como escolher serviços AWS para proteção de dados, foram adicionadas informações sobre AWS Elastic Disaster Recovery. Nas seções Backup e recuperação do Amazon EC2 com snapshots e AMIs, Como preparar um volume do EBS antes de criar um snapshot ou AMI e Como restaurar a partir de um snapshot do Amazon EBS ou de uma AMI acrescent amos mais 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 Como escolher serviços AWS para proteção de dados, serviços foram adicionados. Foi adicionada a seção Backup e recuperação usando o AWS Backup. Na seção Backup e recuperação usando o Amazon S3 e o Amazon S3 Glacier, informações foram adicionadas sobre as novas classes de armazenamento do Amazon S3 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 serviços AWS nativos de nuvem, foi adicionada uma recomendação para uso do AWS Backup. Na seção Recursos adicionais, recursos foram adicionados.	28 de janeiro de 2022

Informações atualizadas	Foram adicionadas informações sobre a configuração de classes de armazenamento à seção Recuperação Flexível do S3 Glacier. Foram adicionadas informações sobre a recuperação de snapshots na seção Backup e recuperação do Amazon EC2 com snapshots e AMIs.	9 de setembro de 2021
Informações atualizadas	Na seção AWS Backup, foram adicionadas informações sobre os serviços AWS que AWS Backup oferece suporte.	1º de junho de 2021
Publicação inicial	—	29 de julho de 2020

AWS Glossário de orientação prescritiva

A seguir estão os termos comumente usados em estratégias, guias e padrões fornecidos pela Orientação AWS Prescritiva. Para sugerir entradas, use o link Fornecer feedback no final do glossário.

Números

7 Rs

Sete estratégias comuns de migração para mover aplicações para a nuvem. Essas estratégias baseiam-se nos 5 Rs identificados pela Gartner em 2011 e consistem em:

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Aurora Edição Compatível com PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: migre seu banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) para Oracle na nuvem. AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migrar seu sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: migre seu banco de dados Oracle local para o Oracle em uma instância do EC2 na nuvem. AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Esse cenário de migração é específico do VMware Cloud on AWS, que oferece suporte à compatibilidade de máquinas virtuais (VM) e à portabilidade da carga de trabalho entre seu ambiente local e. AWSÉ possível usar as tecnologias VMware Cloud Foundation de seus datacenters on-premises ao migrar sua infraestrutura para o VMware

Cloud na AWS. Exemplo: realocar o hipervisor que hospeda seu banco de dados Oracle para o VMware Cloud on. AWS

- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.
- Retirar: desative ou remova aplicações que não são mais necessárias em seu ambiente de origem.

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia (por meio de uma ferramenta de replicação bidirecional ou operações de gravação dupla), e ambos os bancos de dados lidam com transações de aplicações conectadas durante a migração. Esse método oferece suporte à migração em lotes pequenos e controlados, em vez de exigir uma substituição única. É mais flexível, mas exige mais trabalho do que a migração ativa-passiva.

migração ativa-passiva

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia, mas somente o banco de dados de origem manipula as transações das aplicações conectadas enquanto os dados são replicados no banco de dados de destino. O banco de dados de destino não aceita nenhuma transação durante a migração.

função agregada

Uma função SQL que opera em um grupo de linhas e calcula um único valor de retorno para o grupo. Exemplos de funções agregadas incluem `SUM` e. `MAX`

AI

Veja inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

O processo de excluir permanentemente informações pessoais em um conjunto de dados. A anonimização pode ajudar a proteger a privacidade pessoal. Dados anônimos não são mais considerados dados pessoais.

antipadrões

Uma solução frequentemente usada para um problema recorrente em que a solução é contraproducente, ineficaz ou menos eficaz do que uma alternativa.

controle de aplicativos

Uma abordagem de segurança que permite o uso somente de aplicativos aprovados para ajudar a proteger um sistema contra malware.

portfólio de aplicações

Uma coleção de informações detalhadas sobre cada aplicação usada por uma organização, incluindo o custo para criar e manter a aplicação e seu valor comercial. Essas informações são fundamentais para o processo de descoberta e análise de portfólio e ajudam a identificar e priorizar as aplicações a serem migradas, modernizadas e otimizadas.

inteligência artificial (IA)

O campo da ciência da computação que se dedica ao uso de tecnologias de computação para desempenhar funções cognitivas normalmente associadas aos humanos, como aprender, resolver problemas e reconhecer padrões. Para obter mais informações, consulte O que é inteligência artificial?

operações de inteligência artificial (AIOps)

O processo de usar técnicas de machine learning para resolver problemas operacionais, reduzir incidentes operacionais e intervenção humana e aumentar a qualidade do serviço. Para obter

mais informações sobre como as AIOps são usadas na estratégia de migração para a AWS , consulte o guia de integração de operações.

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para descriptografia. É possível compartilhar a chave pública porque ela não é usada na descriptografia, mas o acesso à chave privada deve ser altamente restrito.

atomicidade, consistência, isolamento, durabilidade (ACID)

Um conjunto de propriedades de software que garantem a validade dos dados e a confiabilidade operacional de um banco de dados, mesmo no caso de erros, falhas de energia ou outros problemas.

controle de acesso por atributo (ABAC)

A prática de criar permissões minuciosas com base nos atributos do usuário, como departamento, cargo e nome da equipe. Para obter mais informações, consulte ABAC AWS na documentação AWS Identity and Access Management (IAM).

fonte de dados autorizada

Um local onde você armazena a versão principal dos dados, que é considerada a fonte de informações mais confiável. Você pode copiar dados da fonte de dados autorizada para outros locais com o objetivo de processar ou modificar os dados, como anonimizá-los, redigi-los ou pseudonimizá-los.

Availability Zone (zona de disponibilidade)

Um local distinto dentro de um Região da AWS que está isolado de falhas em outras zonas de disponibilidade e fornece conectividade de rede barata e de baixa latência a outras zonas de disponibilidade na mesma região.

AWS Estrutura de adoção da nuvem (AWS CAF)

Uma estrutura de diretrizes e melhores práticas AWS para ajudar as organizações a desenvolver um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS O CAF organiza a orientação em seis áreas de foco chamadas perspectivas: negócios, pessoas, governança, plataforma, segurança e operações. As perspectivas de negócios, pessoas e governança têm como foco habilidades e processos de negócios; as perspectivas de plataforma, segurança e operações concentram-se em habilidades e processos técnicos. Por exemplo, a perspectiva das pessoas tem como alvo as partes interessadas que lidam com recursos humanos (RH), funções de pessoal e gerenciamento de pessoal. Nessa perspectiva, o AWS CAF fornece orientação para

desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o site da AWS CAF e o whitepaper da AWS CAF.

AWS Estrutura de qualificação da carga de trabalho (AWS WQF)

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS Schema Conversion Tool ()AWS SCT. Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

B

bot ruim

Um bot destinado a perturbar ou causar danos a indivíduos ou organizações.

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

Uma visualização unificada e interativa do comportamento e das interações de recursos ao longo do tempo. É possível usar um gráfico de comportamento com o Amazon Detective para examinar tentativas de login malsucedidas, chamadas de API suspeitas e ações similares. Para obter mais informações, consulte Dados em um gráfico de comportamento na documentação do Detective.

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também endianness.

classificação binária

Um processo que prevê um resultado binário (uma de duas classes possíveis). Por exemplo, seu modelo de ML pode precisar prever problemas como “Este e-mail é ou não é spam?” ou “Este produto é um livro ou um carro?”

filtro de bloom

Uma estrutura de dados probabilística e eficiente em termos de memória que é usada para testar se um elemento é membro de um conjunto.

blue/green deployment (implantação azul/verde)

Uma estratégia de implantação em que você cria dois ambientes separados, mas idênticos. Você executa a versão atual do aplicativo em um ambiente (azul) e a nova versão do aplicativo no outro ambiente (verde). Essa estratégia ajuda você a reverter rapidamente com o mínimo de impacto.

bot

Um aplicativo de software que executa tarefas automatizadas pela Internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como rastreadores da Web que indexam informações na Internet. Alguns outros bots, conhecidos como bots ruins, têm como objetivo perturbar ou causar danos a indivíduos ou organizações.

botnet

Redes de bots infectadas por malware e sob o controle de uma única parte, conhecidas como pastor de bots ou operador de bots. As redes de bots são o mecanismo mais conhecido para escalar bots e seu impacto.

ramo

Uma área contida de um repositório de código. A primeira ramificação criada em um repositório é a ramificação principal. Você pode criar uma nova ramificação a partir de uma ramificação existente e, em seguida, desenvolver recursos ou corrigir bugs na nova ramificação. Uma ramificação que você cria para gerar um recurso é comumente chamada de ramificação de recurso. Quando o recurso estiver pronto para lançamento, você mesclará a ramificação do recurso de volta com a ramificação principal. Para obter mais informações, consulte Sobre filiais (GitHub documentação).

acesso em vidro quebrado

Em circunstâncias excepcionais e por meio de um processo aprovado, um meio rápido para um usuário obter acesso a um Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador Implementar procedimentos de quebra de vidro na orientação do Well-Architected AWS .

estratégia brownfield

A infraestrutura existente em seu ambiente. Ao adotar uma estratégia brownfield para uma arquitetura de sistema, você desenvolve a arquitetura de acordo com as restrições dos sistemas e da infraestrutura atuais. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

cache do buffer

A área da memória em que os dados acessados com mais frequência são armazenados.

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços conteinerizados na AWS.

planejamento de continuidade de negócios (BCP)

Um plano que aborda o impacto potencial de um evento disruptivo, como uma migração em grande escala, nas operações e permite que uma empresa retome as operações rapidamente.

C

CAF

Consulte Estrutura de adoção da AWS nuvem.

implantação canária

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substituirá a versão atual em sua totalidade.

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

captura de dados de alterações (CDC)

O processo de rastrear alterações em uma fonte de dados, como uma tabela de banco de dados, e registrar metadados sobre a alteração. É possível usar o CDC para várias finalidades, como auditar ou replicar alterações em um sistema de destino para manter a sincronização.

engenharia do caos

Introduzir intencionalmente falhas ou eventos disruptivos para testar a resiliência de um sistema. Você pode usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estressam suas AWS cargas de trabalho e avaliar sua resposta.

CI/CD

Veja a integração e a entrega contínuas.

classificação

Um processo de categorização que ajuda a gerar previsões. Os modelos de ML para problemas de classificação predizem um valor discreto. Os valores discretos são sempre diferentes uns dos outros. Por exemplo, um modelo pode precisar avaliar se há ou não um carro em uma imagem.

criptografia no lado do cliente

Criptografia de dados localmente, antes que o alvo os AWS service (Serviço da AWS) receba.

Centro de Excelência da Nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as postagens do CCoE no blog AWS Cloud Enterprise Strategy.

computação em nuvem

A tecnologia de nuvem normalmente usada para armazenamento de dados remoto e gerenciamento de dispositivos de IoT. A computação em nuvem geralmente está conectada à tecnologia de computação de ponta.

modelo operacional em nuvem

Em uma organização de TI, o modelo operacional usado para criar, amadurecer e otimizar um ou mais ambientes de nuvem. Para obter mais informações, consulte Criar seu modelo operacional de nuvem.

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam quando migram para a AWS nuvem:

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação: realizar investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma zona de pouso, definir um CCoE, estabelecer um modelo de operações)
- Migração: migrar aplicações individuais
- Reinvenção: otimizar produtos e serviços e inovar na nuvem

Esses estágios foram definidos por Stephen Orban na postagem do blog The Journey Toward Cloud-First & the Stages of Adoption no blog AWS Cloud Enterprise Strategy. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

Um local onde o código-fonte e outros ativos, como documentação, amostras e scripts, são armazenados e atualizados por meio de processos de controle de versão. Os repositórios de nuvem comuns incluem GitHub ou AWS CodeCommit. Cada versão do código é chamada de ramificação. Em uma estrutura de microsserviços, cada repositório é dedicado a uma única peça de funcionalidade. Um único pipeline de CI/CD pode usar vários repositórios.

cache frio

Um cache de buffer que está vazio, não está bem preenchido ou contém dados obsoletos ou irrelevantes. Isso afeta a performance porque a instância do banco de dados deve ler da memória principal ou do disco, um processo que é mais lento do que a leitura do cache do buffer.

dados frios

Dados que raramente são acessados e geralmente são históricos. Ao consultar esse tipo de dados, consultas lentas geralmente são aceitáveis. Mover esses dados para níveis ou classes de armazenamento de baixo desempenho e menos caros pode reduzir os custos.

visão computacional (CV)

Um campo da IA que usa aprendizado de máquina para analisar e extrair informações de formatos visuais, como imagens e vídeos digitais. Por exemplo, AWS Panorama oferece dispositivos que adicionam CV às redes de câmeras locais, e a Amazon SageMaker fornece algoritmos de processamento de imagem para CV.

desvio de configuração

Para uma carga de trabalho, uma alteração de configuração em relação ao estado esperado. Isso pode fazer com que a carga de trabalho se torne incompatível e, normalmente, é gradual e não intencional.

banco de dados de gerenciamento de configuração (CMDB)

Um repositório que armazena e gerencia informações sobre um banco de dados e seu ambiente de TI, incluindo componentes de hardware e software e suas configurações. Normalmente, os dados de um CMDB são usados no estágio de descoberta e análise do portfólio da migração.

pacote de conformidade

Um conjunto de AWS Config regras e ações de remediação que você pode montar para personalizar suas verificações de conformidade e segurança. Você pode implantar um pacote de conformidade como uma entidade única em uma Conta da AWS região ou em uma organização usando um modelo YAML. Para obter mais informações, consulte Pacotes de conformidade na documentação. AWS Config

integração contínua e entrega contínua (CI/CD)

O processo de automatizar os estágios de origem, criação, teste, preparação e produção do processo de lançamento do software. O CI/CD é comumente descrito como um pipeline. O CI/CD pode ajudar você a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte Benefícios da entrega contínua. CD também pode significar implantação contínua. Para obter mais informações, consulte Entrega contínua versus implantação contínua.

CV

Veja visão computacional.

D

dados em repouso

Dados estacionários em sua rede, por exemplo, dados que estão em um armazenamento.

classificação de dados

Um processo para identificar e categorizar os dados em sua rede com base em criticalidade e confidencialidade. É um componente crítico de qualquer estratégia de gerenciamento de riscos de

segurança cibernética, pois ajuda a determinar os controles adequados de proteção e retenção para os dados. A classificação de dados é um componente do pilar de segurança no AWS Well-Architected Framework. Para obter mais informações, consulte Classificação de dados.

desvio de dados

Uma variação significativa entre os dados de produção e os dados usados para treinar um modelo de ML ou uma alteração significativa nos dados de entrada ao longo do tempo. O desvio de dados pode reduzir a qualidade geral, a precisão e a imparcialidade das previsões do modelo de ML.

dados em trânsito

Dados que estão se movendo ativamente pela sua rede, como entre os recursos da rede.

malha de dados

Uma estrutura arquitetônica que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

minimização de dados

O princípio de coletar e processar apenas os dados estritamente necessários. Praticar a minimização de dados no Nuvem AWS pode reduzir os riscos de privacidade, os custos e a pegada de carbono de sua análise.

perímetro de dados

Um conjunto de proteções preventivas em seu AWS ambiente que ajudam a garantir que somente identidades confiáveis acessem recursos confiáveis das redes esperadas. Para obter mais informações, consulte Construindo um perímetro de dados em. AWS

pré-processamento de dados

A transformação de dados brutos em um formato que seja facilmente analisado por seu modelo de ML. O pré-processamento de dados pode significar a remoção de determinadas colunas ou linhas e o tratamento de valores ausentes, inconsistentes ou duplicados.

proveniência dos dados

O processo de rastrear a origem e o histórico dos dados ao longo de seu ciclo de vida, por exemplo, como os dados foram gerados, transmitidos e armazenados.

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

Um sistema de gerenciamento de dados que oferece suporte à inteligência comercial, como análises. Os data warehouses geralmente contêm grandes quantidades de dados históricos e geralmente são usados para consultas e análises.

linguagem de definição de dados (DDL)

Instruções ou comandos para criar ou modificar a estrutura de tabelas e objetos em um banco de dados.

linguagem de manipulação de dados (DML)

Instruções ou comandos para modificar (inserir, atualizar e excluir) informações em um banco de dados.

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

A combinação de vários modelos de aprendizado profundo para gerar previsões. Os deep ensembles podem ser usados para produzir uma previsão mais precisa ou para estimar a incerteza nas previsões.

Aprendizado profundo

Um subcampo do ML que usa várias camadas de redes neurais artificiais para identificar o mapeamento entre os dados de entrada e as variáveis-alvo de interesse.

defense-in-depth

Uma abordagem de segurança da informação na qual uma série de mecanismos e controles de segurança são cuidadosamente distribuídos por toda a rede de computadores para proteger a confidencialidade, a integridade e a disponibilidade da rede e dos dados nela contidos. Ao adotar essa estratégia AWS, você adiciona vários controles em diferentes camadas da AWS Organizations estrutura para ajudar a proteger os recursos. Por exemplo, uma defense-in-depth abordagem pode combinar autenticação multifatorial, segmentação de rede e criptografia.

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta é chamada de administrador delegado para esse serviço Para obter mais informações e uma

lista de serviços compatíveis, consulte Serviços que funcionam com o AWS Organizations na documentação do AWS Organizations .

implantação

O processo de criar uma aplicação, novos recursos ou correções de código disponíveis no ambiente de destino. A implantação envolve a implementação de mudanças em uma base de código e, em seguida, a criação e execução dessa base de código nos ambientes da aplicação

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

Um controle de segurança projetado para detectar, registrar e alertar após a ocorrência de um evento. Esses controles são uma segunda linha de defesa, alertando você sobre eventos de segurança que contornaram os controles preventivos em vigor. Para obter mais informações, consulte Controles detectivos em Como implementar controles de segurança na AWS.

mapeamento do fluxo de valor de desenvolvimento (DVSM)

Um processo usado para identificar e priorizar restrições que afetam negativamente a velocidade e a qualidade em um ciclo de vida de desenvolvimento de software. O DVSM estende o processo de mapeamento do fluxo de valor originalmente projetado para práticas de manufatura enxuta. Ele se concentra nas etapas e equipes necessárias para criar e movimentar valor por meio do processo de desenvolvimento de software.

gêmeo digital

Uma representação virtual de um sistema real, como um prédio, fábrica, equipamento industrial ou linha de produção. Os gêmeos digitais oferecem suporte à manutenção preditiva, ao monitoramento remoto e à otimização da produção.

tabela de dimensões

Em um esquema em estrela, uma tabela menor que contém atributos de dados sobre dados quantitativos em uma tabela de fatos. Os atributos da tabela de dimensões geralmente são campos de texto ou números discretos que se comportam como texto. Esses atributos são comumente usados para restringir consultas, filtrar e rotular conjuntos de resultados.

desastre

Um evento que impede que uma workload ou sistema cumpra seus objetivos de negócios em seu local principal de implantação. Esses eventos podem ser desastres naturais, falhas técnicas ou o resultado de ações humanas, como configuração incorreta não intencional ou ataque de malware.

recuperação de desastres (DR)

A estratégia e o processo que você usa para minimizar o tempo de inatividade e a perda de dados causados por um desastre. Para obter mais informações, consulte Recuperação de desastres de cargas de trabalho em AWS: Recuperação na nuvem no AWS Well-Architected Framework.

DML

Consulte linguagem de manipulação de banco de dados.

design orientado por domínio

Uma abordagem ao desenvolvimento de um sistema de software complexo conectando seus componentes aos domínios em evolução, ou principais metas de negócios, atendidos por cada componente. Esse conceito foi introduzido por Eric Evans em seu livro, Design orientado por domínio: lidando com a complexidade no coração do software (Boston: Addison-Wesley Professional, 2003). Para obter informações sobre como usar o design orientado por domínio com o padrão strangler fig, consulte Modernizar incrementalmente os serviços web herdados do Microsoft ASP.NET (ASMX) usando contêineres e o Amazon API Gateway.

DR

Veja a recuperação de desastres.

detecção de deriva

Rastreando desvios de uma configuração básica. Por exemplo, você pode usar AWS CloudFormation para detectar desvios nos recursos do sistema ou AWS Control Tower para detectar mudanças em seu landing zone que possam afetar a conformidade com os requisitos de governança.

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

computação de borda

A tecnologia que aumenta o poder computacional de dispositivos inteligentes nas bordas de uma rede de IoT. Quando comparada à computação em nuvem, a computação de ponta pode reduzir a latência da comunicação e melhorar o tempo de resposta.

Criptografia

Um processo de computação que transforma dados de texto simples, legíveis por humanos, em texto cifrado.

chave de criptografia

Uma sequência criptográfica de bits aleatórios que é gerada por um algoritmo de criptografia. As chaves podem variar em tamanho, e cada chave foi projetada para ser imprevisível e exclusiva.

endianismo

A ordem na qual os bytes são armazenados na memória do computador. Os sistemas big-endian armazenam o byte mais significativo antes. Os sistemas little-endian armazenam o byte menos significativo antes.

endpoint

Veja o endpoint do serviço.

serviço de endpoint

Um serviço que pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros diretores Contas da AWS ou a AWS Identity and Access Management (IAM). Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais informações, consulte Criar um serviço de endpoint na documentação do Amazon Virtual Private Cloud (Amazon VPC).

planejamento de recursos corporativos (ERP)

Um sistema que automatiza e gerencia os principais processos de negócios (como contabilidade, MES e gerenciamento de projetos) para uma empresa.

criptografia envelopada

O processo de criptografar uma chave de criptografia com outra chave de criptografia. Para obter mais informações, consulte Criptografia de envelope na documentação AWS Key Management Service (AWS KMS).

environment (ambiente)

Uma instância de uma aplicação em execução. Estes são tipos comuns de ambientes na computação em nuvem:

- ambiente de desenvolvimento: uma instância de uma aplicação em execução que está disponível somente para a equipe principal responsável pela manutenção da aplicação. Ambientes de desenvolvimento são usados para testar mudanças antes de promovê-las para ambientes superiores. Esse tipo de ambiente às vezes é chamado de ambiente de teste.
- ambientes inferiores: todos os ambientes de desenvolvimento para uma aplicação, como aqueles usados para compilações e testes iniciais.
- ambiente de produção: uma instância de uma aplicação em execução que os usuários finais podem acessar. Em um pipeline de CI/CD, o ambiente de produção é o último ambiente de implantação.
- ambientes superiores: todos os ambientes que podem ser acessados por usuários que não sejam a equipe principal de desenvolvimento. Isso pode incluir um ambiente de produção, ambientes de pré-produção e ambientes para testes de aceitação do usuário.

epic

Em metodologias ágeis, categorias funcionais que ajudam a organizar e priorizar seu trabalho. Os epics fornecem uma descrição de alto nível dos requisitos e das tarefas de implementação. Por exemplo, os épicos de segurança AWS da CAF incluem gerenciamento de identidade e acesso, controles de detetive, segurança de infraestrutura, proteção de dados e resposta a incidentes. Para obter mais informações sobre epics na estratégia de migração da AWS , consulte o guia de implementação do programa.

ERP

Consulte planejamento de recursos corporativos.

análise exploratória de dados (EDA)

O processo de analisar um conjunto de dados para entender suas principais características. Você coleta ou agrega dados e, em seguida, realiza investigações iniciais para encontrar padrões,

detectar anomalias e verificar suposições. O EDA é realizado por meio do cálculo de estatísticas resumidas e da criação de visualizações de dados.

F

tabela de fatos

A tabela central em um esquema em estrela. Ele armazena dados quantitativos sobre operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: aquelas que contêm medidas e aquelas que contêm uma chave externa para uma tabela de dimensões.

falham rapidamente

Uma filosofia que usa testes frequentes e incrementais para reduzir o ciclo de vida do desenvolvimento. É uma parte essencial de uma abordagem ágil.

limite de isolamento de falhas

No Nuvem AWS, um limite, como uma zona de disponibilidade, Região da AWS um plano de controle ou um plano de dados, que limita o efeito de uma falha e ajuda a melhorar a resiliência das cargas de trabalho. Para obter mais informações, consulte Limites de isolamento de AWS falhas.

ramificação de recursos

Veja a filial.

recursos

Os dados de entrada usados para fazer uma previsão. Por exemplo, em um contexto de manufatura, os recursos podem ser imagens capturadas periodicamente na linha de fabricação.

importância do recurso

O quanto um recurso é importante para as previsões de um modelo. Isso geralmente é expresso como uma pontuação numérica que pode ser calculada por meio de várias técnicas, como Shapley Additive Explanations (SHAP) e gradientes integrados. Para obter mais informações, consulte Interpretabilidade do modelo de aprendizado de máquina com:AWS.

transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo,

se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

FGAC

Veja o controle de acesso refinado.

controle de acesso refinado (FGAC)

O uso de várias condições para permitir ou negar uma solicitação de acesso.

migração flash-cut

Um método de migração de banco de dados que usa replicação contínua de dados por meio da captura de dados alterados para migrar dados no menor tempo possível, em vez de usar uma abordagem em fases. O objetivo é reduzir ao mínimo o tempo de inatividade.

G

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

Na Amazon CloudFront, uma opção para impedir que usuários em países específicos acessem distribuições de conteúdo. É possível usar uma lista de permissões ou uma lista de bloqueios para especificar países aprovados e banidos. Para obter mais informações, consulte Restringir a distribuição geográfica do seu conteúdo na CloudFront documentação.

Fluxo de trabalho do GitFlow

Uma abordagem na qual ambientes inferiores e superiores usam ramificações diferentes em um repositório de código-fonte. O fluxo de trabalho do Gitflow é considerado legado, e o fluxo de trabalho baseado em troncos é a abordagem moderna e preferida.

estratégia greenfield

A ausência de infraestrutura existente em um novo ambiente. Ao adotar uma estratégia greenfield para uma arquitetura de sistema, é possível selecionar todas as novas tecnologias sem a restrição da compatibilidade com a infraestrutura existente, também conhecida como brownfield. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

barreira de proteção

Uma regra de alto nível que ajuda a gerenciar recursos, políticas e conformidade em todas as unidades organizacionais (UOs). Barreiras de proteção preventivas impõem políticas para garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que usa um mecanismo de banco de dados diferente (por exemplo, Oracle para Amazon Aurora). A migração heterogênea geralmente faz parte de um esforço de redefinição da arquitetura, e converter o esquema pode ser uma tarefa complexa. O AWS fornece o AWS SCT para ajudar nas conversões de esquemas.

alta disponibilidade (HA)

A capacidade de uma workload operar continuamente, sem intervenção, em caso de desafios ou desastres. Os sistemas AH são projetados para realizar o failover automático, oferecer consistentemente desempenho de alta qualidade e lidar com diferentes cargas e falhas com impacto mínimo no desempenho.

modernização de historiador

Uma abordagem usada para modernizar e atualizar os sistemas de tecnologia operacional (OT) para melhor atender às necessidades do setor de manufatura. Um historiador é um tipo de banco de dados usado para coletar e armazenar dados de várias fontes em uma fábrica.

migração homogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que compartilha o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server para Amazon RDS

para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

dados quentes

Dados acessados com frequência, como dados em tempo real ou dados translacionais recentes. Esses dados normalmente exigem uma camada ou classe de armazenamento de alto desempenho para fornecer respostas rápidas às consultas.

hotfix

Uma correção urgente para um problema crítico em um ambiente de produção. Devido à sua urgência, um hotfix geralmente é feito fora do fluxo de trabalho normal de DevOps lançamento.

período de hipercuidados

Imediatamente após a substituição, o período em que uma equipe de migração gerencia e monitora as aplicações migradas na nuvem para resolver quaisquer problemas. Normalmente, a duração desse período é de 1 a 4 dias. No final do período de hipercuidados, a equipe de migração normalmente transfere a responsabilidade pelas aplicações para a equipe de operações de nuvem.

I

IaC

Veja a infraestrutura como código.

Política baseada em identidade

Uma política anexada a um ou mais diretores do IAM que define suas permissões no Nuvem AWS ambiente.

aplicação ociosa

Uma aplicação que tem um uso médio de CPU e memória entre 5 e 20% em um período de 90 dias. Em um projeto de migração, é comum retirar essas aplicações ou retê-las on-premises.

IIoT

Veja a Internet das Coisas industrial.

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que infraestruturas mutáveis. Para obter mais informações, consulte as melhores práticas de implantação usando infraestrutura imutável no Well-Architected AWS Framework.

VPC de entrada (admissão)

Em uma arquitetura de AWS várias contas, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de um aplicativo. A Arquitetura de referência de segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

Um termo que foi introduzido por Klaus Schwab em 2016 para se referir à modernização dos processos de fabricação por meio de avanços em conectividade, dados em tempo real, automação, análise e IA/ML.

infraestrutura

Todos os recursos e ativos contidos no ambiente de uma aplicação.

Infraestrutura como código (IaC)

O processo de provisionamento e gerenciamento da infraestrutura de uma aplicação por meio de um conjunto de arquivos de configuração. A IaC foi projetada para ajudar você a centralizar o gerenciamento da infraestrutura, padronizar recursos e escalar rapidamente para que novos ambientes sejam reproduzíveis, confiáveis e consistentes.

Internet das Coisas Industrial (IIoT)

O uso de sensores e dispositivos conectados à Internet nos setores industriais, como manufatura, energia, automotivo, saúde, ciências biológicas e agricultura. Para obter mais informações,

consulte Construir uma estratégia de transformação digital para a Internet das Coisas Industrial (IIoT).

VPC de inspeção

Em uma arquitetura de AWS várias contas, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (na mesma ou em diferentes Regiões da AWS), a Internet e as redes locais. A Arquitetura de referência de segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

Internet das Coisas (IoT)

A rede de objetos físicos conectados com sensores ou processadores incorporados que se comunicam com outros dispositivos e sistemas pela Internet ou por uma rede de comunicação local. Para obter mais informações, consulte O que é IoT?

interpretabilidade

Uma característica de um modelo de machine learning que descreve o grau em que um ser humano pode entender como as previsões do modelo dependem de suas entradas. Para obter mais informações, consulte Interpretabilidade do modelo de machine learning com a AWS.

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

Um conjunto de práticas recomendadas para fornecer serviços de TI e alinhar esses serviços a requisitos de negócios. A ITIL fornece a base para o ITSM.

Gerenciamento de serviços de TI (ITSM)

Atividades associadas a design, implementação, gerenciamento e suporte de serviços de TI para uma organização. Para obter informações sobre a integração de operações em nuvem com ferramentas de ITSM, consulte o guia de integração de operações.

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

: Uma implementação do controle de acesso obrigatório (MAC) em que os usuários e os dados em si recebem explicitamente um valor de etiqueta de segurança. A interseção entre a etiqueta de segurança do usuário e a etiqueta de segurança dos dados determina quais linhas e colunas podem ser vistas pelo usuário.

zona de pouso

: Uma landing zone é um AWS ambiente bem arquitetado, com várias contas, escalável e seguro. Um ponto a partir do qual suas organizações podem iniciar e implantar rapidamente workloads e aplicações com confiança em seu ambiente de segurança e infraestrutura. Para obter mais informações sobre zonas de pouso, consulte Configurar um ambiente da AWS com várias contas seguro e escalável.

migração de grande porte

: Uma migração de 300 servidores ou mais.

LBAC

: Veja controle de acesso baseado em etiquetas.

privilégio mínimo

: A prática recomendada de segurança de conceder as permissões mínimas necessárias para executar uma tarefa. Para obter mais informações, consulte Aplicar permissões de privilégios mínimos na documentação do IAM.

mover sem alterações (lift-and-shift)

: Veja 7 Rs.

sistema little-endian

: Um sistema que armazena o byte menos significativo antes. Veja também endianness.

ambientes inferiores

: Veja o ambiente.

M

machine learning (ML)

Um tipo de inteligência artificial que usa algoritmos e técnicas para reconhecimento e aprendizado de padrões. O ML analisa e aprende com dados gravados, por exemplo, dados da Internet das Coisas (IoT), para gerar um modelo estatístico baseado em padrões. Para obter mais informações, consulte Machine learning.

ramificação principal

Veja a filial.

malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vazar informações confidenciais ou obter acesso não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Tróia, spyware e keyloggers.

serviços gerenciados

Serviços da AWS para o qual AWS opera a camada de infraestrutura, o sistema operacional e as plataformas, e você acessa os endpoints para armazenar e recuperar dados. O Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB são exemplos de serviços gerenciados. Eles também são conhecidos como serviços abstratos.

sistema de execução de manufatura (MES)

Um sistema de software para rastrear, monitorar, documentar e controlar processos de produção que convertem matérias-primas em produtos acabados no chão de fábrica.

MAP

Consulte Migration Acceleration Program.

mecanismo

Um processo completo no qual você cria uma ferramenta, impulsiona a adoção da ferramenta e, em seguida, inspeciona os resultados para fazer ajustes. Um mecanismo é um ciclo que se reforça e se aprimora à medida que opera. Para obter mais informações, consulte Construindo mecanismos no AWS Well-Architected Framework.

conta-membro

Todos, Contas da AWS exceto a conta de gerenciamento, que fazem parte de uma organização em AWS Organizations. Uma conta só pode ser membro de uma organização de cada vez.

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens (MQTT)

Um protocolo de comunicação leve machine-to-machine (M2M), baseado no padrão de publicação/assinatura, para dispositivos de IoT com recursos limitados.

microsserviço

Um serviço pequeno e independente que se comunica por meio de APIs bem definidas e normalmente pertence a equipes pequenas e autônomas. Por exemplo, um sistema de seguradora pode incluir microsserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos microsserviços incluem agilidade, escalabilidade flexível, fácil implantação, código reutilizável e resiliência. Para obter mais informações, consulte Integração de microsserviços usando serviços sem AWS servidor.

arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio de uma interface bem definida usando APIs leves. Cada microsserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte Implementação de microsserviços em. AWS

Programa de Aceleração da Migração (MAP)

Um AWS programa que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a compensar o custo inicial das migrações. O MAP inclui uma metodologia de migração para executar migrações legadas de forma metódica e um conjunto de ferramentas para automatizar e acelerar cenários comuns de migração.

migração em escala

O processo de mover a maior parte do portfólio de aplicações para a nuvem em ondas, com mais aplicações sendo movidas em um ritmo mais rápido a cada onda. Essa fase usa as práticas

recomendadas e lições aprendidas nas fases anteriores para implementar uma fábrica de migração de equipes, ferramentas e processos para agilizar a migração de workloads por meio de automação e entrega ágeis. Esta é a terceira fase da estratégia de migração para a AWS.

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações, analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte discussão sobre fábricas de migração e o guia do Cloud Migration Factory neste conjunto de conteúdo.

metadados de migração

As informações sobre a aplicação e o servidor necessárias para concluir a migração. Cada padrão de migração exige um conjunto de metadados de migração diferente. Exemplos de metadados de migração incluem a sub-rede, o grupo de segurança e AWS a conta de destino.

padrão de migração

Uma tarefa de migração repetível que detalha a estratégia de migração, o destino da migração e a aplicação ou o serviço de migração usado. Exemplo: rehospede a migração para o Amazon EC2 AWS com o Application Migration Service.

Avaliação de Portfólio para Migração (MPA)

Uma ferramenta on-line que fornece informações para validar o caso de negócios para a migração para a AWS nuvem. O MPA fornece avaliação detalhada do portfólio (dimensionamento correto do servidor, preços, comparações de TCO, análise de custos de migração), bem como planejamento de migração (análise e coleta de dados de aplicações, agrupamento de aplicações, priorização de migração e planejamento de ondas). A ferramenta MPA (requer login) está disponível gratuitamente para todos os AWS consultores e consultores parceiros da APN.

Avaliação de Preparação para Migração (MRA)

O processo de obter insights sobre o status de prontidão de uma organização para a nuvem, identificar pontos fortes e fracos e criar um plano de ação para fechar as lacunas identificadas, usando o CAF. AWS Para mais informações, consulte o guia de preparação para migração. A MRA é a primeira fase da estratégia de migração para a AWS.

estratégia de migração

A abordagem usada para migrar uma carga de trabalho para a AWS nuvem. Para obter mais informações, consulte a entrada de 7 Rs neste glossário e consulte Mobilize sua organização para acelerar migrações em grande escala.

ML

Veja o aprendizado de máquina.

modernização

Transformar uma aplicação desatualizada (herdada ou monolítica) e sua infraestrutura em um sistema ágil, elástico e altamente disponível na nuvem para reduzir custos, ganhar eficiência e aproveitar as inovações. Para obter mais informações, consulte Estratégia para modernizar aplicativos no Nuvem AWS.

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte Avaliar a preparação para modernização de aplicações na AWS Cloud.

aplicações monolíticas (monólitos)

Aplicações que são executadas como um único serviço com processos fortemente acoplados. As aplicações monolíticas apresentam várias desvantagens. Se um recurso da aplicação apresentar um aumento na demanda, toda a arquitetura deverá ser escalada. Adicionar ou melhorar os recursos de uma aplicação monolítica também se torna mais complexo quando a base de código cresce. Para resolver esses problemas, é possível criar uma arquitetura de microsserviços. Para obter mais informações, consulte Decompor monólitos em microsserviços.

MAPA

Consulte Avaliação do portfólio de migração.

MQTT

Consulte Transporte de telemetria de enfileiramento de mensagens.

classificação multiclasse

Um processo que ajuda a gerar previsões para várias classes (prevendo um ou mais de dois resultados). Por exemplo, um modelo de ML pode perguntar “Este produto é um livro, um carro ou um telefone?” ou “Qual categoria de produtos é mais interessante para este cliente?”

infraestrutura mutável

Um modelo que atualiza e modifica a infraestrutura existente para cargas de trabalho de produção. Para melhorar a consistência, confiabilidade e previsibilidade, o AWS Well-Architected Framework recomenda o uso de infraestrutura imutável como uma prática recomendada.

O

OAC

Veja o controle de acesso de origem.

CARVALHO

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

Um método de migração no qual a workload de origem é desativada durante o processo de migração. Esse método envolve tempo de inatividade prolongado e geralmente é usado para workloads pequenas e não críticas.

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

Um método de migração no qual a workload de origem é copiada para o sistema de destino sem ser colocada offline. As aplicações conectadas à workload podem continuar funcionando durante a migração. Esse método envolve um tempo de inatividade nulo ou mínimo e normalmente é usado para workloads essenciais para a produção.

OPC-UA

Consulte Comunicação de processo aberto — Arquitetura unificada.

Comunicação de processo aberto — Arquitetura unificada (OPC-UA)

Um protocolo de comunicação machine-to-machine (M2M) para automação industrial. O OPC-UA fornece um padrão de interoperabilidade com esquemas de criptografia, autenticação e autorização de dados.

acordo de nível operacional (OLA)

Um acordo que esclarece o que os grupos funcionais de TI prometem oferecer uns aos outros para apoiar um acordo de serviço (SLA).

análise de prontidão operacional (ORR)

Uma lista de verificação de perguntas e melhores práticas associadas que ajudam você a entender, avaliar, prevenir ou reduzir o escopo de incidentes e possíveis falhas. Para obter mais informações, consulte Operational Readiness Reviews (ORR) no Well-Architected AWS Framework.

tecnologia operacional (OT)

Sistemas de hardware e software que funcionam com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas OT e de tecnologia da informação (TI) é o foco principal das transformações da Indústria 4.0.

integração de operações (OI)

O processo de modernização das operações na nuvem, que envolve planejamento de preparação, automação e integração. Para obter mais informações, consulte o guia de integração de operações.

trilha organizacional

Uma trilha criada por ela AWS CloudTrail registra todos os eventos de todos Contas da AWS em uma organização em AWS Organizations. Essa trilha é criada em cada Conta da AWS que faz parte da organização e monitora a atividade em cada conta. Para obter mais informações, consulte Criação de uma trilha para uma organização na CloudTrail documentação.

gerenciamento de alterações organizacionais (OCM)

Uma estrutura para gerenciar grandes transformações de negócios disruptivas de uma perspectiva de pessoas, cultura e liderança. O OCM ajuda as organizações a se prepararem

e fazerem a transição para novos sistemas e estratégias, acelerando a adoção de alterações, abordando questões de transição e promovendo mudanças culturais e organizacionais. Na estratégia de AWS migração, essa estrutura é chamada de aceleração de pessoas, devido à velocidade de mudança exigida nos projetos de adoção da nuvem. Para obter mais informações, consulte o guia do OCM.

controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo do Amazon Simple Storage Service (Amazon S3). O OAC oferece suporte a todos os buckets S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e solicitações dinâmicas ao bucket S3. `PUT` `DELETE`

Identidade do acesso de origem (OAI)

Em CloudFront, uma opção para restringir o acesso para proteger seu conteúdo do Amazon S3. Quando você usa o OAI, CloudFront cria um principal com o qual o Amazon S3 pode se autenticar. Os diretores autenticados podem acessar o conteúdo em um bucket do S3 somente por meio de uma distribuição específica. CloudFront Veja também OAC, que fornece um controle de acesso mais granular e aprimorado.

OU

Veja a análise de prontidão operacional.

NÃO

Veja a tecnologia operacional.

VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A Arquitetura de referência de segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

P

limite de permissões

Uma política de gerenciamento do IAM anexada a entidades principais do IAM para definir as permissões máximas que o usuário ou perfil podem ter. Para obter mais informações, consulte Limites de permissões na documentação do IAM.

informações de identificação pessoal (PII)

Informações que, quando visualizadas diretamente ou combinadas com outros dados relacionados, podem ser usadas para inferir razoavelmente a identidade de um indivíduo. Exemplos de PII incluem nomes, endereços e informações de contato.

PII

Veja as informações de identificação pessoal.

manual

Um conjunto de etapas predefinidas que capturam o trabalho associado às migrações, como a entrega das principais funções operacionais na nuvem. Um manual pode assumir a forma de scripts, runbooks automatizados ou um resumo dos processos ou etapas necessários para operar seu ambiente modernizado.

PLC

Consulte controlador lógico programável.

AMEIXA

Veja o gerenciamento do ciclo de vida do produto.

política

Um objeto que pode definir permissões (consulte a política baseada em identidade), especificar as condições de acesso (consulte a política baseada em recursos) ou definir as permissões máximas para todas as contas em uma organização em AWS Organizations (consulte a política de controle de serviços).

persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um microsserviço com base em padrões de acesso a dados e outros requisitos. Se seus microsserviços tiverem a mesma tecnologia de armazenamento de dados, eles poderão enfrentar desafios de implementação ou apresentar baixa performance. Os microsserviços serão implementados com mais facilidade e alcançarão performance e escalabilidade melhores se usarem o armazenamento de dados mais bem adaptado às suas necessidades. Para obter mais informações, consulte Habilitar a persistência de dados em microsserviços.

avaliação do portfólio

Um processo de descobrir, analisar e priorizar o portfólio de aplicações para planejar a migração. Para obter mais informações, consulte Avaliar a preparação para a migração.

predicado

Uma condição de consulta que retorna `true` ou`false`, normalmente localizada em uma `WHERE` cláusula.

pressão de predicados

Uma técnica de otimização de consulta de banco de dados que filtra os dados na consulta antes da transferência. Isso reduz a quantidade de dados que devem ser recuperados e processados do banco de dados relacional e melhora o desempenho das consultas.

controle preventivo

Um controle de segurança projetado para evitar que um evento ocorra. Esses controles são a primeira linha de defesa para ajudar a evitar acesso não autorizado ou alterações indesejadas em sua rede. Para obter mais informações, consulte Controles preventivos em Como implementar controles de segurança na AWS.

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais informações, consulte Entidade principal em Termos e conceitos de perfis na documentação do IAM.

Privacidade por design

Uma abordagem em engenharia de sistemas que leva em consideração a privacidade em todo o processo de engenharia.

zonas hospedadas privadas

Um contêiner que armazena informações sobre como você quer que o Amazon Route 53 responda a consultas ao DNS para um domínio e seus subdomínios dentro de uma ou mais VPCs. Para obter mais informações, consulte Como trabalhar com zonas hospedadas privadas na documentação do Route 53.

controle proativo

Um controle de segurança projetado para impedir a implantação de recursos não compatíveis. Esses controles examinam os recursos antes de serem provisionados. Se o recurso não estiver em conformidade com o controle, ele não será provisionado. Para obter mais informações, consulte o guia de referência de controles na AWS Control Tower documentação e consulte Controles proativos em Implementação de controles de segurança em AWS.

gerenciamento do ciclo de vida do produto (PLM)

O gerenciamento de dados e processos de um produto em todo o seu ciclo de vida, desde o design, desenvolvimento e lançamento, passando pelo crescimento e maturidade, até o declínio e a remoção.

ambiente de produção

Veja o ambiente.

controlador lógico programável (PLC)

Na fabricação, um computador altamente confiável e adaptável que monitora as máquinas e automatiza os processos de fabricação.

pseudonimização

O processo de substituir identificadores pessoais em um conjunto de dados por valores de espaço reservado. A pseudonimização pode ajudar a proteger a privacidade pessoal. Os dados pseudonimizados ainda são considerados dados pessoais.

publicar/assinar (pub/sub)

Um padrão que permite comunicações assíncronas entre microsserviços para melhorar a escalabilidade e a capacidade de resposta. Por exemplo, em um MES baseado em microsserviços, um microsserviço pode publicar mensagens de eventos em um canal no qual outros microsserviços possam se inscrever. O sistema pode adicionar novos microsserviços sem alterar o serviço de publicação.

Q

plano de consulta

Uma série de etapas, como instruções, usadas para acessar os dados em um sistema de banco de dados relacional SQL.

regressão de planos de consultas

Quando um otimizador de serviço de banco de dados escolhe um plano menos adequado do que escolhia antes de uma determinada alteração no ambiente de banco de dados ocorrer. Isso pode ser causado por alterações em estatísticas, restrições, configurações do ambiente, associações de parâmetros de consulta e atualizações do mecanismo de banco de dados.

R

Matriz RACI

Veja responsável, responsável, consultado, informado (RACI).

ransomware

Um software mal-intencionado desenvolvido para bloquear o acesso a um sistema ou dados de computador até que um pagamento seja feito.

Matriz RASCI

Veja responsável, responsável, consultado, informado (RACI).

RCAC

Veja o controle de acesso por linha e coluna.

réplica de leitura

Uma cópia de um banco de dados usada somente para leitura. É possível encaminhar consultas para a réplica de leitura e reduzir a carga no banco de dados principal.

rearquiteta

Veja 7 Rs.

objetivo de ponto de recuperação (RPO)

Período de tempo aceitável máximo desde o último ponto de recuperação de dados. Determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

objetivo de tempo de recuperação (RTO)

O atraso máximo aceitável entre a interrupção e a restauração do serviço.

refatorar

Veja 7 Rs.

Região

Uma coleção de AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter mais informações, consulte Especificar o que Regiões da AWS sua conta pode usar.

regressão

Uma técnica de ML que prevê um valor numérico. Por exemplo, para resolver o problema de “Por qual preço esta casa será vendida?” um modelo de ML pode usar um modelo de regressão linear para prever o preço de venda de uma casa com base em fatos conhecidos sobre a casa (por exemplo, a metragem quadrada).

redefinir a hospedagem

Veja 7 Rs.

versão

Em um processo de implantação, o ato de promover mudanças em um ambiente de produção.

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

A capacidade de um aplicativo de resistir ou se recuperar de interrupções. Alta disponibilidade e recuperação de desastres são considerações comuns ao planejar a resiliência no. Nuvem AWS Para obter mais informações, consulte Nuvem AWS Resiliência.

política baseada em recurso

Uma política associada a um recurso, como um bucket do Amazon S3, um endpoint ou uma chave de criptografia. Esse tipo de política especifica quais entidades principais têm acesso permitido, ações válidas e quaisquer outras condições que devem ser atendidas.

matriz responsável, accountable, consultada, informada (RACI)

Uma matriz que define as funções e responsabilidades de todas as partes envolvidas nas atividades de migração e nas operações de nuvem. O nome da matriz é derivado dos tipos de responsabilidade definidos na matriz: responsável (R), responsabilizável (A), consultado (C) e informado (I). O tipo de suporte (S) é opcional. Se você incluir suporte, a matriz será chamada de matriz RASCI e, se excluir, será chamada de matriz RACI.

controle responsivo

Um controle de segurança desenvolvido para conduzir a remediação de eventos adversos ou desvios em relação à linha de base de segurança. Para obter mais informações, consulte Controles responsivos em Como implementar controles de segurança na AWS.

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

rotação

O processo de atualizar periodicamente um segredo para dificultar o acesso das credenciais por um invasor.

controle de acesso por linha e coluna (RCAC)

O uso de expressões SQL básicas e flexíveis que tenham regras de acesso definidas. O RCAC consiste em permissões de linha e máscaras de coluna.

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

Um conjunto de procedimentos manuais ou automatizados necessários para realizar uma tarefa específica. Eles são normalmente criados para agilizar operações ou procedimentos repetitivos com altas taxas de erro.

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login AWS Management Console ou chamar as operações da AWS API sem que você precise criar um usuário no IAM para todos

em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte Sobre a federação baseada em SAML 2.0 na documentação do IAM.

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele consiste no valor secreto e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte Secret na documentação do Secrets Manager.

controle de segurança

Uma barreira de proteção técnica ou administrativa que impede, detecta ou reduz a capacidade de uma ameaça explorar uma vulnerabilidade de segurança. Existem quatro tipos principais de controles de segurança: preventivos, detectivos, responsivos e proativos.

fortalecimento da segurança

O processo de reduzir a superfície de ataque para torná-la mais resistente a ataques. Isso pode incluir ações como remover recursos que não são mais necessários, implementar a prática recomendada de segurança de conceder privilégios mínimos ou desativar recursos desnecessários em arquivos de configuração.

sistema de gerenciamento de eventos e informações de segurança (SIEM)

Ferramentas e serviços que combinam sistemas de gerenciamento de informações de segurança (SIM) e gerenciamento de eventos de segurança (SEM). Um sistema SIEM coleta, monitora e analisa dados de servidores, redes, dispositivos e outras fontes para detectar ameaças e violações de segurança e gerar alertas.

automação de resposta de segurança

Uma ação predefinida e programada projetada para responder ou remediar automaticamente um evento de segurança. Essas automações servem como controles de segurança responsivos ou detectivos que ajudam você a implementar as melhores práticas AWS de segurança. Exemplos de ações de resposta automatizada incluem a modificação de um grupo de segurança da VPC, a correção de uma instância do Amazon EC2 ou a rotação de credenciais.

Criptografia do lado do servidor

Criptografia dos dados em seu destino, por AWS service (Serviço da AWS) quem os recebe.

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização no AWS Organizations. As SCPs definem barreiras de proteção ou estabelecem limites para as ações que um administrador pode delegar a usuários ou perfis. É possível usar SCPs como listas de permissão ou de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte Políticas de controle de serviço na AWS Organizations documentação.

service endpoint (endpoint de serviço)

O URL do ponto de entrada para um AWS service (Serviço da AWS). Você pode usar o endpoint para se conectar programaticamente ao serviço de destino. Para obter mais informações, consulte Endpoints do AWS service (Serviço da AWS) na Referência geral da AWS.

acordo de serviço (SLA)

Um acordo que esclarece o que uma equipe de TI promete fornecer aos clientes, como tempo de atividade e performance do serviço.

indicador de nível de serviço (SLI)

Uma medida de um aspecto de desempenho de um serviço, como taxa de erro, disponibilidade ou taxa de transferência.

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme medida por um indicador de nível de serviço.

modelo de responsabilidade compartilhada

Um modelo que descreve a responsabilidade com a qual você compartilha AWS pela segurança e conformidade na nuvem. AWS é responsável pela segurança da nuvem, enquanto você é responsável pela segurança na nuvem. Para obter mais informações, consulte o Modelo de responsabilidade compartilhada.

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

Uma falha em um único componente crítico de um aplicativo que pode interromper o sistema.

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte Abordagem em fases para modernizar aplicativos no. Nuvem AWS

CUSPE

Veja um único ponto de falha.

esquema de estrelas

Uma estrutura organizacional de banco de dados que usa uma grande tabela de fatos para armazenar dados transacionais ou medidos e usa uma ou mais tabelas dimensionais menores para armazenar atributos de dados. Essa estrutura foi projetada para uso em um data warehouse ou para fins de inteligência comercial.

padrão strangler fig

Uma abordagem à modernização de sistemas monolíticos que consiste em reescrever e substituir incrementalmente a funcionalidade do sistema até que o sistema herdado possa ser desativado. Esse padrão usa a analogia de uma videira que cresce e se torna uma árvore estabelecida e, eventualmente, supera e substitui sua hospedeira. O padrão foi apresentado por Martin Fowler como forma de gerenciar riscos ao reescrever sistemas monolíticos. Para ver um exemplo de como aplicar esse padrão, consulte Modernizar incrementalmente os serviços Web herdados do Microsoft ASP.NET (ASMX) usando contêineres e o Amazon API Gateway.

sub-rede

Um intervalo de endereços IP na VPC. Uma sub-rede deve residir em uma única zona de disponibilidade.

controle de supervisão e aquisição de dados (SCADA)

Na manufatura, um sistema que usa hardware e software para monitorar ativos físicos e operações de produção.

symmetric encryption (criptografia simétrica)

Um algoritmo de criptografia que usa a mesma chave para criptografar e descriptografar dados.

testes sintéticos

Testar um sistema de forma que simule as interações do usuário para detectar possíveis problemas ou monitorar o desempenho. Você pode usar o Amazon CloudWatch Synthetics para criar esses testes.

T

tags

Pares de valores-chave que atuam como metadados para organizar seus recursos. AWS As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar recursos. Para obter mais informações, consulte Marcar seus recursos do AWS.

variável-alvo

O valor que você está tentando prever no ML supervisionado. Ela também é conhecida como variável de resultado. Por exemplo, em uma configuração de fabricação, a variável-alvo pode ser um defeito do produto.

lista de tarefas

Uma ferramenta usada para monitorar o progresso por meio de um runbook. Uma lista de tarefas contém uma visão geral do runbook e uma lista de tarefas gerais a serem concluídas. Para cada tarefa geral, ela inclui o tempo estimado necessário, o proprietário e o progresso.

ambiente de teste

Veja o ambiente.

treinamento

O processo de fornecer dados para que seu modelo de ML aprenda. Os dados de treinamento devem conter a resposta correta. O algoritmo de aprendizado descobre padrões nos dados de treinamento que mapeiam os atributos dos dados de entrada no destino (a resposta que você deseja prever). Ele gera um modelo de ML que captura esses padrões. Você pode usar o modelo de ML para obter previsões de novos dados cujo destino você não conhece.

gateway de trânsito

Um hub de trânsito de rede que pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações, consulte O que é um gateway de trânsito na AWS Transit Gateway documentação.

fluxo de trabalho baseado em troncos

Uma abordagem na qual os desenvolvedores criam e testam recursos localmente em uma ramificação de recursos e, em seguida, mesclam essas alterações na ramificação principal. A ramificação principal é então criada para os ambientes de desenvolvimento, pré-produção e produção, sequencialmente.

Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas de gerenciamento para você. Para obter mais informações, consulte Usando AWS Organizations com outros AWS serviços na AWS Organizations documentação.

tuning (ajustar)

Alterar aspectos do processo de treinamento para melhorar a precisão do modelo de ML. Por exemplo, você pode treinar o modelo de ML gerando um conjunto de rótulos, adicionando rótulos e repetindo essas etapas várias vezes em configurações diferentes para otimizar o modelo.

equipe de duas pizzas

Uma pequena DevOps equipe que você pode alimentar com duas pizzas. Uma equipe de duas pizzas garante a melhor oportunidade possível de colaboração no desenvolvimento de software.

U

incerteza

Um conceito que se refere a informações imprecisas, incompletas ou desconhecidas que podem minar a confiabilidade dos modelos preditivos de ML. Há dois tipos de incertezas: a incerteza epistêmica é causada por dados limitados e incompletos, enquanto a incerteza aleatória é causada pelo ruído e pela aleatoriedade inerentes aos dados. Para obter mais informações, consulte o guia Como quantificar a incerteza em sistemas de aprendizado profundo.

tarefas indiferenciadas

Também conhecido como trabalho pesado, trabalho necessário para criar e operar um aplicativo, mas que não fornece valor direto ao usuário final nem oferece vantagem competitiva. Exemplos de tarefas indiferenciadas incluem aquisição, manutenção e planejamento de capacidade.

ambientes superiores

Veja o ambiente.

V

aspiração

Uma operação de manutenção de banco de dados que envolve limpeza após atualizações incrementais para recuperar armazenamento e melhorar a performance.

controle de versões

Processos e ferramentas que rastreiam mudanças, como alterações no código-fonte em um repositório.

emparelhamento de VPC

Uma conexão entre duas VPCs que permite rotear tráfego usando endereços IP privados. Para ter mais informações, consulte O que é emparelhamento de VPC? na documentação da Amazon VPC.

vulnerabilidade

Uma falha de software ou hardware que compromete a segurança do sistema.

W

cache quente

Um cache de buffer que contém dados atuais e relevantes que são acessados com frequência. A instância do banco de dados pode ler do cache do buffer, o que é mais rápido do que ler da memória principal ou do disco.

dados mornos

Dados acessados raramente. Ao consultar esse tipo de dados, consultas moderadamente lentas geralmente são aceitáveis.

função de janela

Uma função SQL que executa um cálculo em um grupo de linhas que se relacionam de alguma forma com o registro atual. As funções de janela são úteis para processar tarefas, como calcular uma média móvel ou acessar o valor das linhas com base na posição relativa da linha atual.

workload

Uma coleção de códigos e recursos que geram valor empresarial, como uma aplicação voltada para o cliente ou um processo de back-end.

workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte o AWS Workload Qualification Framework.

escreva uma vez, leia muitas (WORM)

Um modelo de armazenamento que grava dados uma única vez e evita que os dados sejam excluídos ou modificados. Os usuários autorizados podem ler os dados quantas vezes forem

necessárias, mas não podem alterá-los. Essa infraestrutura de armazenamento de dados é considerada imutável.

Z

exploração de dia zero

Um ataque, geralmente malware, que tira proveito de uma vulnerabilidade de dia zero.

vulnerabilidade de dia zero

Uma falha ou vulnerabilidade não mitigada em um sistema de produção. Os agentes de ameaças podem usar esse tipo de vulnerabilidade para atacar o sistema. Os desenvolvedores frequentemente ficam cientes da vulnerabilidade como resultado do ataque.

aplicação zumbi

Uma aplicação que tem um uso médio de CPU e memória inferior a 5%. Em um projeto de migração, é comum retirar essas aplicações.

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.