



Estratégia de recuperação de desastres para bancos de dados em AWS

AWS Recomendações



AWS Recomendações: Estratégia de recuperação de desastres para bancos de dados em AWS

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

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

Table of Contents

Introdução	1
Resultados de negócios desejados	4
Reduzir as perdas financeiras	4
Reduzir o impacto em processos comerciais críticos	4
Reduzir a coordenação manual durante um evento real (automação)	4
Reter seus clientes	4
Aprimorar a segurança	5
Aumentar a produtividade dos funcionários	5
Definir a estratégia de DR	6
Escolhendo um serviço de banco de dados	10
Impulsionar a adoção da estratégia de DR	14
Automatizar sua estratégia de DR	15
Detecção de eventos de desastre	15
Failover	15
Testar para conquistar confiança	17
Considerações	17
Frequência de teste	17
Detecção de desvios	18
Observabilidade	18
Próximas etapas e recursos	19
Histórico do documento	20
.....	xxii

Estratégia de recuperação de desastres para bancos de dados em AWS

Oliver Francis, Balaji Desikachari, Jitendra Kumar e Suhas Basavaraj, da Amazon Web Services

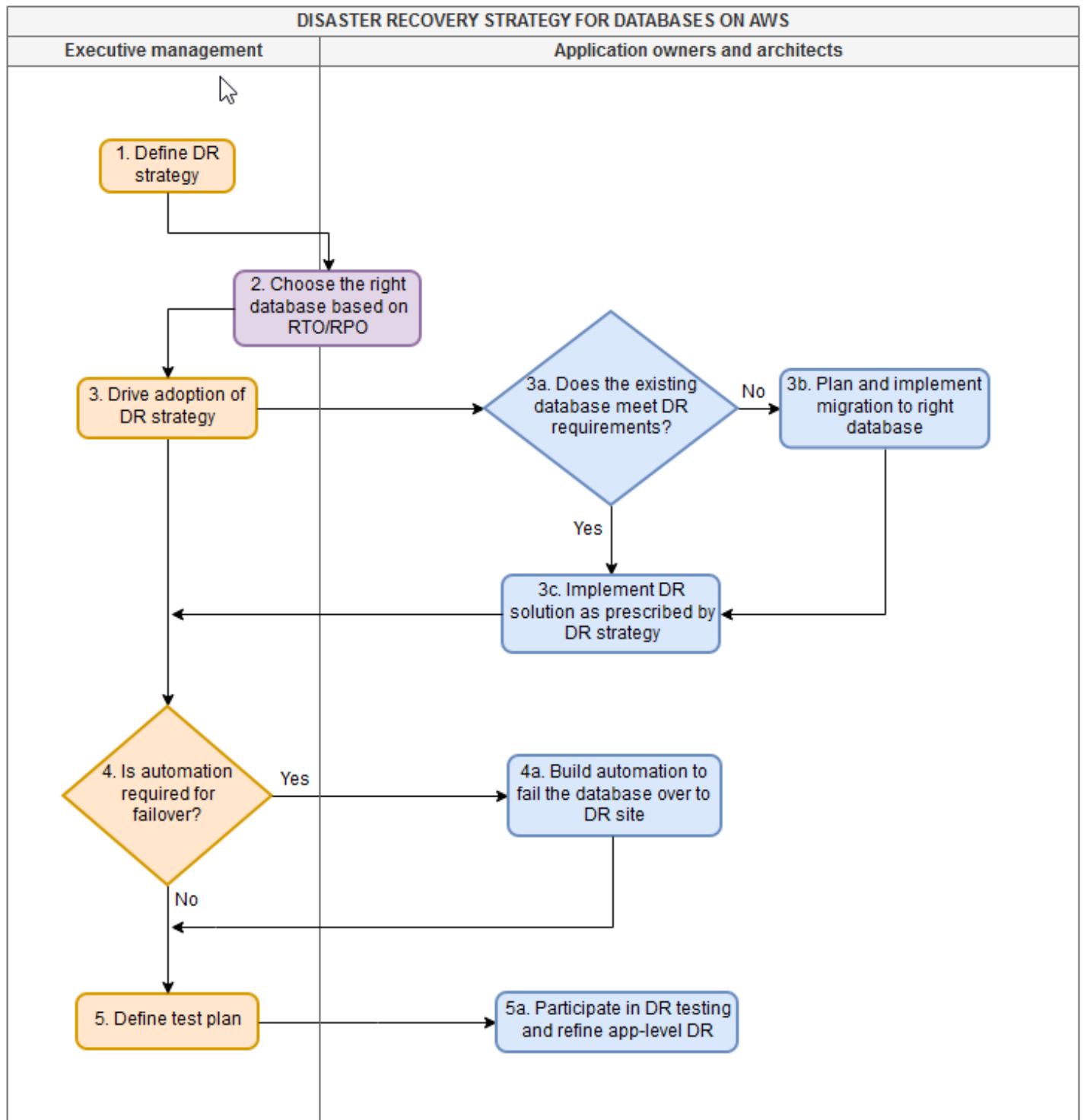
Em outubro de 2021, o Forbes Technology Council publicou um artigo intitulado [Por que a recuperação de desastres não é mais opcional para as empresas atuais](#). O artigo cita uma U.S. Estudo da Agência Federal de Gerenciamento de Emergências (FEMA) que afirma que 40% das pequenas e médias empresas nos Estados Unidos da América fecham após um desastre. Além disso, 25% das empresas que reabrem fecham novamente em um ano. Considerando a gravidade do assunto, um plano de continuidade de negócios bem preparado que inclua uma estratégia de recuperação de desastres (DR) para ativos de TI é crucial para garantir o crescimento e o sucesso dos seus negócios a longo prazo. A computação em nuvem tornou a recuperação de desastres viável até mesmo para pequenas e médias empresas ao reduzir a barreira de entrada. Considerando os riscos decorrentes da falta de uma solução adequada no caso de um desastre, um plano de continuidade de negócios que inclua uma estratégia de DR deve estar no topo da sua lista de prioridades como líder de negócios.

Se suas cargas de trabalho estão sendo executadas AWS, sem dúvida, a maior parte dos seus dados reside em AWS bancos de dados. Sejam dados armazenados em um sistema de banco de dados relacional (RDBMS), como o Amazon Aurora Edition, MySQL-Compatible ou em um banco de dados NoSQL, como o Amazon DynamoDB, esses dados são valiosos para sua empresa. O desenvolvimento de uma estratégia de DR específica para bancos de dados AWS ajuda você a entender o que AWS oferece em termos de recuperação de desastres para seus bancos de dados e como você pode aproveitar essas informações em seu plano de DR para Nuvem AWS o.

O diagrama de raia de natação a seguir apresenta tarefas de alto nível associadas à definição e à implementação de uma estratégia de DR. As duas colunas mostram as tarefas pertencentes à equipe de gerenciamento executivo e as tarefas pertencentes a proprietários e arquitetos de aplicações. A equipe de gerenciamento executivo é responsável pela tomada de decisões. Essa equipe define a estratégia de DR a ser seguida pela organização, impulsiona a adoção da DR em toda a organização, decide se a automação será necessária para atingir as metas de DR e define o plano de teste de DR.

Quando a estratégia de DR entra em vigor, a equipe de gerenciamento executivo trabalha com os proprietários e arquitetos de aplicações para escolher os bancos de dados certos que atendam às expectativas de objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO)

derivadas da estratégia de DR. À medida que a equipe de gerenciamento executivo impulsiona a adoção da estratégia de DR, os proprietários e arquitetos de aplicativos avaliam os bancos de dados usados em seus aplicativos e migram para o banco de dados correto se os atuais não atingirem o RTO e o RPO definidos para o aplicativo. Os proprietários e arquitetos de aplicações também criam automação, se necessário, e participam dos testes de DR para refinar e melhorar a DR em nível de aplicação.



Este artigo explica essas etapas em alto nível para líderes de negócios e tomadores de decisões que desejam formular uma estratégia de DR entre regiões que ajude a atingir seus objetivos comerciais. O artigo pressupõe algum conhecimento técnico e familiaridade com a terminologia de recuperação de desastres, mas nenhuma experiência. AWS

Resultados de negócios desejados

Esta seção discute os resultados esperados associados à definição e à criação de um plano de recuperação de desastres (DR) para seus bancos de dados na AWS.

Reduzir as perdas financeiras

Se você tiver uma solução de DR bem projetada para bancos de dados que armazenam os dados da sua aplicação, poderá se recuperar de eventos catastróficos com mais rapidez e com o mínimo ou nenhuma perda de dados. Isso minimiza as perdas financeiras que podem resultar da indisponibilidade da aplicação por períodos prolongados ou, na pior das hipóteses, da perda permanente dos dados.

Reduzir o impacto em processos comerciais críticos

Ao identificar seus serviços e processos de nível 0 e planejar sua estratégia de DR para recuperá-los rapidamente, você poderá reduzir impactos significativos nesses serviços e processos e também lidar com a recuperação de processos dependentes.

Reduzir a coordenação manual durante um evento real (automação)

Se você optar por automatizar sua solução de DR, poderá reduzir a coordenação manual necessária para executar a solução de DR em caso de evento de desastre. A automação é benéfica mesmo quando você está testando seu [plano de continuidade de negócios \(BCP\)](#), que especifica como você sustenta as operações comerciais padrão durante uma interrupção não planejada.

Reter seus clientes

Em um mercado competitivo, sua estratégia de DR afeta a forma como você conquista a fidelidade e retém clientes. Se sua organização tem a capacidade de se recuperar rapidamente de desastres, é possível criar confiança com seus clientes.

Aprimorar a segurança

Uma estratégia bem planejada de DR entre regiões pode ajudar a restringir o impacto de um ataque de ransomware a uma Região da AWS e permitir que você use seus dados em outra região livremente sem perder seus dados.

Aumentar a produtividade dos funcionários

Se seus funcionários entenderem bem o processo de DR e se sentirem confortáveis com ele, um evento de DR não causará pânico. Você pode seguir runbooks bem definidos para implementar a solução de DR, e seus funcionários podem fazer o melhor uso do tempo para que sua empresa volte ao normal.

Definindo sua estratégia de recuperação de desastres

Dependendo da importância das aplicações em sua organização para seus negócios, é possível decidir por uma estratégia uniforme para todas as aplicações ou desenvolver uma estratégia de DR mais complexa com base na criticidade de cada aplicação. Sua organização pode tolerar um tempo de inatividade de várias horas antes que todas as aplicações sejam disponibilizadas no site de DR. Nesse caso, você poderá optar por uma estratégia econômica de DR baseada em backup e restauração para todos os bancos de dados. Por outro lado, os negócios de sua organização podem depender da rápida disponibilização de alguns serviços ou aplicações essenciais, com requisitos mais agressivos de RPO e RTO, enquanto outras aplicações podem tolerar necessidades menos rigorosas de RPO e RTO. Nesse caso, será necessário atribuir a estratégia de DR correta para cada nível de aplicações e bancos de dados.

A tabela a seguir descreve quatro opções de DR para cargas de trabalho executadas no Nuvem AWS, para ajudá-lo a determinar e definir a estratégia de DR da sua organização. O RPO e o RTO documentados nesta tabela referem-se a uma pilha completa que inclui componentes de aplicação e de banco de dados. Para obter mais informações, consulte [Opções de recuperação de desastres na nuvem](#) na documentação do AWS Well-Architected Framework. A próxima seção aborda as opções de RPO e RTO que são específicas para bancos de dados.

Opção de recuperação	RPO	RTO	Tarefas de infraestrutura na região de DR	Custo
Backup e restauração	Horas	Menos de 24 horas	Provisione todos os recursos de aplicações necessários na região de DR e restaure o banco de dados a partir de um snapshot copiado.	Baixo
Luz piloto	Dezenas de minutos	Dezenas de minutos	Provisione uma cópia da sua	Médio

infraestrutura de aplicações e desative os recursos na pilha de aplicações. Replique seus dados de uma região para outra. Mantenha os bancos de dados sempre ativos e sincronizados com os bancos de dados primários. Provisione os recursos sob demanda durante o evento de failover e teste. Também é necessário implantar alterações na infraestrutura e nas aplicações nas duas regiões simultaneamente. É possível simplificar isso por meio da criação de pipelines de automação que podem sincronizar código e

infraestrutura
nas regiões
primária e de
DR.

Standby morno

Minutos

Minutos

Provisione uma
cópia de toda a
infraestrutura de
aplicações na
região de DR,
mas mantenha
a cópia reduzida
em comparaçã
o com a região
principal. A
região de DR
poderá aceitar
tráfego em um
volume menor
em comparaçã
o com a região
primária.

Alto

Multi-site or active/active	Perto de zero	Zero ou quase zero	Provisione uma cópia completa da infraestr utura na região de DR. Todos os recursos na região de DR serão equivalentes aos recursos da região principal e poderão atender ao tráfego na mesma escala da região principal. Como não há interrupç ão no fluxo de tráfego, essa opção não exige uma tarefa de failover como parte do plano de DR.	Mais alto
--------------------------------	---------------	-----------------------	---	-----------

Escolher o o banco de dados certo para seus requisitos de RTO e RPO

Depois de definir a estratégia de DR para sua organização com base na tabela da seção anterior, escolha os bancos de dados adequados aos seus requisitos de RPO e RTO. Por padrão, todos os serviços AWS de banco de dados oferecem funcionalidade de backup e restauração. Use a tabela a seguir para entender os recursos de DR mais avançados fornecidos pelos serviços de banco de dados da AWS e mapeie-os de acordo com seus requisitos de DR.

AWS serviço de banco de dados	Método de replicação para a região de DR	Possível classificação em standby	RTO	RPO
Amazon RDS para MySQL	Cross-Region réplica de leitura	1. Luz piloto 2. Standby morno com capacidade de leitura de tráfego	Normalmente, minutos. A automação pode minimizar os atrasos.	Normalmente, menos de 1 segundo
Amazon RDS para PostgreSQL	Cross-Region réplica de leitura	1. Luz piloto 2. Standby morno com capacidade de leitura de tráfego	Normalmente, minutos. A automação pode minimizar os atrasos.	Normalmente, menos de 1 segundo
Amazon RDS para MariaDB	Cross-Region réplica de leitura	1. Luz piloto 2. Standby morno com capacidade de leitura de tráfego	Normalmente, minutos. A automação pode minimizar os atrasos.	Normalmente, menos de 1 segundo
Edição Amazon Aurora MySQL-Compatible	O banco de dados global tem clusters secundários	1. Hot standby com capacidade de suportar tráfego de leitura 2. Standby	Normalmente, menos de 1 minuto.	Normalmente, menos de 1 segundo

	em uma região diferente	morno com suporte a tráfego de leitura		
Edição Amazon Aurora PostgreSQL-Compatible	O banco de dados global tem clusters secundários em uma região diferente	1. Hot standby com capacidade de suportar tráfego de leitura 2. Standby morno com suporte a tráfego de leitura	Normalmente, menos de 1 minuto.	Normalmente, menos de 1 segundo
Amazon DocumentDB (compatível com MongoDB)	O cluster global tem clusters secundários em uma região diferente	1. Hot standby com capacidade de suportar tráfego de leitura 2. Standby morno com suporte a tráfego de leitura	Normalmente, menos de 1 minuto.	Em segundos
Amazon ElastiCache (Redis OSS)	O datastore global tem um cluster secundário em uma região diferente	1. Hot standby com capacidade de suportar tráfego de leitura 2. Standby morno com suporte a tráfego de leitura	Normalmente, minutos. A automação pode minimizar os atrasos.	Em segundos
Amazon DynamoDB	Tabelas globais do DynamoDB	Active/active a configuração aceita operações de gravação na região secundária	Zero ou quase zero.	Sub-second

Amazon RDS para Oracle	Promoção de réplicas de leitura em todas as regiões (Oracle Enterprise Edition e Active Data Guard)	1. Luz piloto 2. Standby morno com capacidade de leitura de tráfego	Normalmente, minutos.	Normalmente, menos de 1 segundo
Amazon RDS para Oracle (alternativa)	Promoção de réplicas de leitura montadas entre as regiões (Oracle Enterprise Edition e Active Data Guard)	1. Luz piloto 2. Standby morno (não permite consultas de leitura)	Normalmente, minutos.	Normalmente, menos de 1 segundo
Amazon RDS para SQL Server	Cross-Region réplica de leitura (Microsoft SQL Server Enterprise Edition 2016-2022)	1. Luz piloto 2. Standby morno com capacidade de leitura de tráfego	Normalmente, minutos. A automação pode minimizar os atrasos.	Normalmente, menos de 1 segundo
Amazon Neptune	O banco de dados global tem clusters secundários em uma região diferente	1. Hot standby com capacidade de suportar tráfego de leitura 2. Standby morno com suporte a tráfego de leitura	Normalmente, menos de 1 minuto.	Normalmente 1 segundo

Amazon RDS para Db2	Cross-Region réplica de leitura (Amazon RDS para Db2 11.5.9 e 12.1.4)	1. Luz piloto 2. Standby morno com capacidade de leitura de tráfego	Normalmente, minutos. A automação pode minimizar os atrasos.	Normalmente, menos de 1 segundo
Amazon MemoryDBMulti-Region	Multi-Region cluster com replicação ativa-ativa	Active/active a configuração aceita operações de gravação na região secundária	Zero ou quase zero.	Normalmente, menos de 1 segundo

Impulsionando a adoção de sua estratégia de recuperação de desastres

Quando sua estratégia de DR está implementada, é possível impulsionar a adoção da estratégia em toda a organização. Quando ela atingir 100% de adoção, todas as aplicações e seus bancos de dados estarão em condições de lidar com um evento adverso de DR e poderão atingir a maturidade de DR por meio de testes.

Você pode trabalhar com proprietários e arquitetos de aplicativos para impulsionar a adoção comunicando a estratégia de DR em toda a organização e solicitando que os funcionários avaliem os bancos de dados atuais da AWS usados em seus aplicativos. Isso garante que todos os bancos de dados usados no momento possam atender às expectativas definidas na estratégia de DR. Se os proprietários e arquitetos de aplicativos determinarem que o banco de dados que escolheram para seus aplicativos não pode atender aos requisitos da estratégia de DR, eles terão que planejar uma migração para um AWS banco de dados adequado que possa atingir as expectativas de RTO e RPO escolhidas. Por exemplo, se uma aplicação crítica em sua empresa que exige um RPO em segundos e um RTO em minutos usa no momento uma instância de banco de dados do Amazon RDS para Oracle, o Amazon RDS não conseguirá atender a essas expectativas. Nesse caso, você pode considerar migrar a carga de trabalho para o [Amazon PostgreSQL-Compatible Aurora](#) e usar um banco de dados global para atender às expectativas definidas pela sua estratégia de DR.

Automatizando sua estratégia de recuperação de desastres

Opcionalmente, escolha entre implementar a automação total ou parcial para obter um melhor controle da recuperação de desastres. Se você estiver usando a opção DR de backup e restauração, poderá automatizar seus backups usando, que oferece suporte a todos os bancos de dados do Amazon RDS [AWS Backup](#), bem como às tabelas do DynamoDB, Amazon DocumentDB e Amazon Neptune.

Detecção de eventos de desastre

Para reduzir o tempo de recuperação, considere automatizar a detecção de um evento regional, que pode então iniciar o failover para a região de DR. Para implementar a detecção automatizada para obter um RTO agressivo, você pode criar uma solução baseada em [verificações de integridade](#). Essas verificações de integridade não param nos heartbeats (que verificam se os módulos do ambiente de gerenciamento e do plano de dados em uma rede podem se comunicar entre si), mas avaliam mais profundamente a natureza inter-relacionada dos componentes da aplicação para chegar a uma previsão precisa. No entanto, uma solução automatizada pode acarretar o risco de alarmes falsos, o que pode levar a failovers desnecessários. Tenha cuidado nesse caso, pois failovers desnecessários introduzem problemas de disponibilidade para sua empresa. Você também pode criar substituições manuais no fluxo de trabalho para confirmar que o failover foi realizado. Assine o feed RSS [Service Health Dashboard](#) para se manter em dia com as interrupções em nível de serviço. Além disso, você pode usar o [AWS Health Painel](#) (requer um Conta da AWS) em sua região e conta principais para ficar ciente dos eventos que podem afetar sua conta. Isso pode ajudá-lo a tomar uma decisão informada de falhar no caso de um Region-wide evento.

Failover

Independentemente da estratégia de DR escolhida, é possível criar soluções personalizadas de automação de DR para realizar o failover na região de DR. Essa automação pode minimizar a necessidade de intervenção manual e fornecer maior controle no teste da sua solução de DR. Você pode escolher entre as [APIs de AWS serviço, que são](#) AWS fornecidas em várias linguagens JavaScript, como Python, PHP, .NET, Ruby, Java, Go e C++ Node.js, com base na preferência da sua organização. Para criar uma automação que use essas APIs de AWS serviço, você deve primeiro se concentrar em transformar a infraestrutura do banco de dados em código na forma de modelos do AWS CloudFormation Terraform. Esses modelos podem ajudar a automatizar o failover

de vários bancos de dados e também manter a ordem na qual os componentes da aplicação e do banco de dados são reativados na região de DR.

Para fins de DR, recomendamos se concentrar nesses dois objetivos:

- As [CloudFormation pilhas existentes devem exportar](#) informações pertinentes sobre seus bancos de dados, incluindo nomes de instâncias e endpoints. Seus processos de automação podem se referir a esses valores de exportação dentro de uma região e realizar operações que serão úteis para suas operações de DR.
- Se você tem recursos em produção, mas não tem uma CloudFormation pilha associada, você deve se concentrar em criar pilhas para esses recursos. Certifique-se também de que essas pilhas cubram os valores de exportação corretos, conforme mencionado no ponto anterior.

Depois de atingir essas duas metas, você pode criar soluções de automação no idioma de sua organização para aproveitar CloudFormation as exportações e executar automaticamente as ações de transição necessárias no caso de um desastre. Por exemplo, se você tiver um armazenamento de dados global ElastiCache (Redis OSS) implantado como CloudFormation modelo, o código de automação terá acesso às CloudFormation exportações que fornecem detalhes sobre o armazenamento de dados global. No caso de um desastre, o código pode promover automaticamente o armazenamento de dados secundário para o armazenamento de dados primário sem qualquer intervenção manual usando as APIs de serviço ElastiCache (Redis OSS).

Em um cenário típico, a automação deve ser escalável para vários bancos de dados em sua organização. É possível escalar suas soluções de automação para vários bancos de dados usando [AWS Step Functions](#) ou [AWS Batch](#).

Testar para conquistar confiança

A melhor solução de DR para bancos de dados é aquela que é testada com frequência e passa pelas seguintes verificações:

- Recuperação adequada de dados que atende às expectativas de RPO de cada banco de dados
- Restauração completa de um banco de dados em funcionamento dentro do prazo de RTO esperado, o que permite que as aplicações se conectem ao banco de dados e retomem a funcionalidade completa

Os testes de DR devem fazer parte de sua estratégia de negócios para que os backups funcionem quando se fazem mais necessários. O teste de DR também deve abordar casos em que:

- O tamanho de um banco de dados cresceu significativamente, e sua estratégia atual de DR não atende mais ao acordo de serviço (SLA) da empresa.
- Um arquivo de backup está corrompido, o que poderia causar problemas durante a recuperação.

O que considerar ao testar sua estratégia de DR

- Tenha metas claras de continuidade de negócios em relação ao RPO e ao RTO e certifique-se de que os resultados dos testes estejam alinhados às suas metas.
- Crie um plano de teste de DR detalhado que leve em consideração os requisitos financeiros e de recursos humanos para o teste.
- Atribua recursos para documentar possíveis problemas e aprendizados.
- Atualize sua estratégia de DR com base nos aprendizados e encontre a solução que ofereça suporte aos processos e à automação ideais que funcionam para sua organização.

Frequência de testes para soluções de DR

Não há recomendações definidas para os ciclos de teste de DR, a menos que elas sejam explicitamente prescritas por regulamentações. Por exemplo, a auditoria de conformidade com os Payment Card Industry Data Security Standards (PCI DSS) exige que as organizações testem seu plano de DR pelo menos uma vez por ano. (Consulte os [requisitos de recuperação de desastres do PCI DSS](#) no site do PCI DSS.)

As equipes de aplicações também podem realizar testes contínuos de suas soluções individuais de DR quando a aplicação ou a infraestrutura mudam.

Detecção de desvios

Sua solução de DR também deve lidar com a [detecção de desvios](#). Isso garantirá que a região principal e a região de DR estejam no nível certo de sincronização e garantirá um bom progresso durante os testes. O [AWS Config](#) fornece gerenciamento de configuração e rastreamento histórico de configurações em sua infraestrutura e pode ajudar a gerenciar o desvio de forma eficaz.

Observabilidade

Melhorar a observabilidade afeta positivamente sua preparação para os testes. Todas as soluções de DR movem dados da região primária para a região secundária (DR). Você pode configurar alertas para atrasos de replicação e backups, ou implementar um processo para realizar verificações diárias que garantam que seus dados foram copiados com êxito para a região de DR.

Próximas etapas e recursos

- Para obter mais informações sobre DR em AWS, leia o white paper [Recuperação de Desastres de Cargas de Trabalho em AWS: Recuperação na nuvem](#).
- Analise o [pilare de confiabilidade](#) na AWS Well-Architected Estrutura.
- Explore [AWS Resilience Hub](#) para monitorar e validar a resiliência de suas AWS cargas de trabalho.
- Analise os seguintes recursos adicionais:
 - [Usar o failover em um Amazon Aurora Global Database](#) (documentação do Aurora)
 - [Replicação Regiões da AWS usando armazenamentos de dados globais \(documentação da Amazon ElastiCache \(Redis OSS\)\)](#)
 - [Recuperação de desastres e clusters globais do Amazon DocumentDB](#) (documentação do Amazon DocumentDB)
 - [Prepare-se para uma recuperação de desastres mais rápida: implante um banco de dados global Amazon Aurora com o Terraform \(Parte 1\) \(AWS postagem do blog\)](#)
 - [Tabelas globais do Amazon DynamoDB \(site\)](#) AWS
 - [Recuperação de desastres](#) ativada AWS, [Cross-Region replicação](#) (laboratório Amazon RDS)
 - [Cross-Region recuperação de desastres do Amazon RDS para SQL Server](#) AWS (postagem no blog)
 - [Recuperação gerenciada de desastres com o Amazon RDS for Oracle Backups automatizados entre regiões — Parte 1](#) AWS (postagem no blog)

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia.

Alteração	Descrição	Data
Detalhes atualizados na tabela de comparação	A seção Escolhendo o banco de dados certo para seus requisitos de RTO e RPO foi atualizada.	29 de junho de 2026
Detalhes atualizados na tabela de comparação	Na seção Escolhendo o banco de dados certo para seus requisitos de RTO e RPO , atualizou as informações sobre o Amazon RDS for Db2 e corrigiu os detalhes do RPO para Amazon RDS for Oracle e Amazon RDS for Oracle (alternativa).	11 de junho de 2025
Adicionado o Amazon RDS para Db2	Na seção Escolhendo o banco de dados certo para seus requisitos de RTO e RPO , foram adicionadas informações sobre o Amazon RDS for Db2.	4 de março de 2024
RTO/RPO Detalhes atualizados	Na seção Escolhendo o banco de dados certo para seus requisitos de RTO e RPO , atualizou as informações sobre Amazon DocumentDB, ElastiCache Amazon (Redis OSS) e Amazon RDS for SQL Server.	19 de abril de 2023

Publicação inicial

—

26 de outubro de 2022

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.