
Abordagem da Amazon Web Services à resiliência operacional no setor financeiro e além

Março de 2019



[Guia de recursos]



© 2020 Amazon Web Services, Inc. ou suas afiliadas. Todos os direitos reservados.

Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento. Este documento (a) é fornecido apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não cria nenhum compromisso ou garantia da AWS e suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos no "estado em que se encontram", sem qualquer garantia, declaração ou condição de qualquer tipo, explícita ou implícita. As responsabilidades e obrigações da AWS com seus clientes são regidas por contratos da AWS, e este documento não modifica nem faz parte de nenhum contrato entre a AWS e seus clientes.



Sumário

| | |
|--|----------|
| Introdução | 1 |
| A resiliência operacional é uma responsabilidade compartilhada..... | 1 |
| Como a AWS mantém a resiliência operacional e a continuidade do serviço | 2 |
| Gerenciamento de incidentes..... | 4 |
| Clientes podem alcançar e testar a resiliência na AWS | 5 |
| Primeiros princípios | 5 |
| Dos princípios de design à implementação | 7 |
| Mecanismos de garantia e conformidade..... | 9 |
| Verificação independente de terceiros..... | 9 |
| Garantia direta para clientes | 10 |



Introdução

A Amazon Web Services (AWS) fornece serviços de tecnologia da informação (TI) e elementos básicos para todos os tipos de empresas, autoridades públicas, universidades e indivíduos que utilizam nossos serviços para se tornarem mais seguros, inovadores e responsivos às suas próprias necessidades e às de seus clientes. A AWS oferece serviços de TI em categorias que variam de computação, armazenamento, banco de dados e rede a inteligência artificial e machine learning. A AWS padroniza seus serviços e os disponibiliza a todos os clientes, incluindo instituições financeiras. Em todo o mundo, as instituições financeiras usam os serviços da AWS para criarem suas próprias aplicações de serviços bancários para dispositivos móveis, relatórios normativos e análises de mercado.

A finalidade deste artigo é descrever como a AWS e nossos clientes no setor de serviços financeiros alcançam a resiliência operacional usando os serviços da AWS. O público-alvo principal deste artigo são as organizações interessadas em como a AWS e os nossos clientes de serviços financeiros podem operar os serviços diante de mudanças constantes, que vão

Qual o significado da resiliência operacional na AWS?

Resiliência operacional é a capacidade de fornecer serviço contínuo por meio de pessoas, processos e tecnologia que estejam cientes das mudanças constantes e sejam capazes de se adaptar a elas. Esta é uma prática incorporada à cultura da AWS, orientada à execução em tempo real, que é diferente das abordagens tradicionais em Continuidade de negócios, Recuperação de desastres e Gerenciamento de crises, que dependem principalmente de programas hierárquicos centralizados com foco no desenvolvimento e na manutenção da documentação.

desde pequenos eventos climáticos a problemas cibernéticos. A AWS e o setor de serviços financeiros compartilham o interesse comum de manter a resiliência operacional, ou seja, a capacidade de fornecer serviço contínuo apesar das interrupções. A continuidade do serviço, especialmente para funções econômicas críticas, é um pré-requisito essencial para a estabilidade financeira. A AWS reconhece que as instituições financeiras que usam os serviços da AWS precisam cumprir as obrigações regulatórias específicas do setor e os requisitos internos relacionados à resiliência operacional.

Essas obrigações e requisitos são encontrados, entre outras, nas diretrizes¹ de TI e nas orientações de resiliência cibernética². As instituições financeiras podem confiar na AWS para o fornecimento de infraestrutura e serviços resilientes, enquanto arquitetam aplicações

que atendam às obrigações regulatórias e de conformidade. Essa abordagem dupla da resiliência operacional é algo que chamamos de “responsabilidade compartilhada”.

A resiliência operacional é uma responsabilidade compartilhada

A AWS é responsável por garantir que os serviços usados por nossos clientes – os componentes básicos para suas aplicações – estejam disponíveis continuamente, além de assegurar que estejamos preparados para lidar com uma ampla gama de eventos que podem afetar nossa infraestrutura.

Neste documento, também exploramos a responsabilidade dos clientes pela resiliência operacional, como os clientes podem projetar, implantar e testar suas aplicações na AWS para obter a disponibilidade e a resiliência que precisam, inclusive para as aplicações de missão crítica que exigem quase nenhum tempo de inatividade.

¹ Por exemplo, Manual de TI do Federal Financial Institution Examination Council (FFIEC). Consulte-o em <https://ithandbook.ffiec.gov>.

² Por exemplo, Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions (CPMI-IOSCO), *Orientação sobre resiliência cibernética para infraestruturas do mercado financeiro* (junho de 2016). Consulte-a em <https://www.bis.org/cpmi/publ/d146.pdf>.



Esses tipos de aplicações exigem que a infraestrutura e os serviços da AWS estejam disponíveis quando os clientes precisarem deles, mesmo na ocorrência de uma interrupção. Conforme discutido abaixo, os clientes podem usar os serviços da AWS para projetar aplicações que atendam a esse padrão e fornecer um nível de segurança e resiliência que consideramos superiores ao que os ambientes de TI locais (on-premises) podem oferecer..

Por fim, dada a importância da resiliência operacional para nossos clientes, também exploramos a variedade de mecanismos que a AWS oferece aos clientes para demonstrar conformidade.³

Como a AWS mantém a resiliência operacional e a continuidade do serviço

A nuvem AWS é construída visando se proteger contra interrupções de serviço e incidentes, assim como também levamos em consideração no design de nossos serviços. Portanto, quando ocorrem interrupções, o impacto sobre os clientes e a continuidade dos serviços é o menor possível. Para evitar pontos únicos de falha, a AWS minimiza a interconectividade em nossa infraestrutura global. A infraestrutura global da AWS está geograficamente dispersa em cinco continentes. É composta de 24 regiões geográficas, compostas por 76 Availability Zones (AZs – Zonas de disponibilidade) que, por sua vez, são compostas por datacenters (Figura 1)⁴ As AZs, fisicamente separadas e independentes umas das outras, também são criadas com redes altamente redundantes para resistir a interrupções locais. As regiões estão isoladas umas das outras, o que significa que uma interrupção em uma região não resulta em propagação nas outras regiões. Em comparação com os ambientes locais (on-premises) das instituições financeiras globais hoje em dia, a diversidade local da infraestrutura da AWS reduz bastante o risco de concentração geográfica. Estamos adicionando continuamente novas regiões e AZs. Você pode ver nosso mapa de infraestrutura global mais atual aqui: <https://aws.amazon.com/about-aws/global-infrastructure>.

Na AWS, empregamos técnicas para compartimentar toda a nossa infraestrutura e serviços. Temos vários blocos construtivos que fornecem diferentes camadas de componentes independentes e redundantes. Começando em um alto nível, considere nossas regiões. Para minimizar a interconectividade, a AWS implanta uma pilha dedicada de infraestrutura e serviços em cada região. As regiões são autônomas e isoladas umas das outras, apesar de permitirmos que os clientes repliquem dados e executem operações entre as regiões. Para tornar possível o uso de recursos entre regiões, a AWS toma muito cuidado em garantir que as dependências e os padrões de chamadas entre regiões sejam assíncronos e protegidos por mecanismos de segurança. Por exemplo, projetamos o Amazon Simple Storage Service (Amazon S3) para permitir que os clientes repliquem dados de uma região (por exemplo, US-EAST-1) para outra região (por exemplo, US-WEST-1). Contudo, também projetamos o S3 para operar de forma autônoma em cada região,

³ Observação: este documento reflete apenas uma visão geral dos nossos esforços contínuos para garantir que nossos clientes possam usar os serviços da AWS de forma segura. Para complementar nosso conceito de responsabilidade compartilhada, também nos dedicamos a superar as expectativas normativas e dos clientes. Para essa finalidade, as equipes técnicas, os arquitetos de segurança e os especialistas em conformidade da AWS ajudam as instituições financeiras a atender aos requisitos normativos e internos, inclusive com a demonstração ativa da segurança e resiliência deles por meio de monitoramento, correção e testes contínuos. A AWS engaja continuamente com reguladores financeiros em todo o mundo para explicar como a infraestrutura e os serviços da AWS permitem que instituições financeiras de todos os portes e tipos, desde startups de tecnologia financeira até bolsas de valores, melhorem a segurança e a resiliência em comparação ao ambiente no local (on-premises). Sempre queremos receber feedback dos clientes e seus reguladores sobre a abordagem da AWS e as suas experiências.

⁴ Você pode fazer um tour virtual em um datacenter da AWS aqui: <https://aws.amazon.com/compliance/data-center>



Região e número de zonas de disponibilidade

US East

N. Virginia (6),
Ohio (3)

US West

N. California (3),
Oregon (4)

Asia Pacific

Mumbai (2),
Seoul (2),
Singapore (3),
Sydney (3),
Tokyo (4),
Osaka-Local (1)¹

Canada

Central (2)

China

Beijing (2),
Ningxia (3)

Europe

Frankfurt (3),
Ireland (3),
London (3),
Paris (3),
Stockholm (3)

South America

São Paulo (3)

GovCloud (US)

US-East (3),
US-West (3)



Nova região (em breve)

Bahrain

Cape Town

Hong Kong SAR

Milan

Figura 1. Infraestrutura global da AWS



para que uma interrupção do S3 no US-EAST não resulte em uma interrupção do S3 no US-WEST.⁵ A grande maioria dos serviços opera em sua totalidade dentro de uma única região. As poucas exceções a essa abordagem envolvem serviços que fornecem entrega global, como o Amazon Route 53 (nosso serviço de DNS - sigla em inglês de Sistema de Nome de Domínio), cujo plano de dados é projetado para 100% de disponibilidade. Conforme discutido abaixo, as instituições financeiras e outros clientes podem criar arquiteturas em várias regiões assim como em várias zonas de disponibilidade.

As zonas de disponibilidade são compostas por vários datacenters que formam uma região e demonstram maior compartimentalização. A localização de AZs em uma mesma região permite a replicação de dados (redundância) sem um impacto substancial na latência, um benefício importante para instituições financeiras e outros clientes que precisam de baixa latência para executar suas aplicações. Ao mesmo tempo, garantimos que as AZs sejam independentes para garantir que os serviços continuem disponíveis em caso de incidentes graves. As AZs têm infraestrutura física independente e estão distantes entre si para mitigar os efeitos de incêndios, inundações e outros eventos. Muitos serviços da AWS são executados de forma autônoma nas AZs. Isso significa que, se uma AZ dentro de uma única região perder energia ou conectividade, as outras AZs naquela região não serão afetadas ou, no caso de um erro de software, o risco de propagação desse erro seja limitado. A independência entre AZs permite que a AWS crie serviços regionais usando várias AZs que, por sua vez, fornecem alta disponibilidade e resiliência aos nossos clientes.

Além disso, a AWS aproveita outro conceito conhecido como arquitetura baseada em célula. As células são várias instâncias de um serviço que ficam isoladas umas das outras. Essas estruturas internas de serviço são invisíveis para os clientes. Em uma arquitetura baseada em célula, os recursos e as solicitações são particionados em células, cujo tamanho é limitado. Esse design minimiza a chance de uma interrupção em uma célula – por exemplo, em um subconjunto de clientes – interromper outras células. Ao reduzir a amplitude de impacto (blast radius) de uma determinada falha em um serviço baseado em células, a disponibilidade geral aumenta e a continuidade do serviço permanece. Uma analogia grosseira é um conjunto de anteparas estanques (divisórias impermeáveis) em um navio: anteparas suficientes, projetadas adequadamente, podem conter água caso o casco do navio se rompa e permitirão que o navio permaneça flutuando.

Gerenciamento de incidentes

Embora a probabilidade de tais incidentes seja muito baixa, a AWS está preparada para gerenciar eventos de larga escala que afetam nossa infraestrutura e nossos serviços. A AWS toma conhecimento de incidentes ou degradações no serviço com base no monitoramento contínuo de métricas e alarmes, tíquetes de alta gravidade, notificações de clientes e linhas diretas de serviço e suporte técnico que operam ininterruptamente (24 horas por dia, 7 dias por semana, 365 dias ao ano). No caso de um evento significativo, um engenheiro de plantão convoca uma chamada com os agentes encarregados de solucionar problemas para analisar o evento e determinar se outros agentes devem ser acionados. O líder de plantão conduz o grupo de agentes solucionadores a encontrar a causa raiz e mitigar o evento. Os agentes solucionadores relevantes executarão as ações necessárias para solucionar o evento. Após encaminhar a solução do problema (troubleshooting), os procedimentos de reparo e os componentes afetados, o líder de plantão atribuirá documentação e ações de acompanhamento e encerrará a conexão da chamada. O líder de plantão irá declarar a fase de recuperação concluída após as atividades de correção

⁵ Conforme evidenciado pela interrupção do serviço Amazon S3 de 28 de fevereiro de 2017, que ocorreu na região norte da Virgínia (US-EAST-1), mas não em outras regiões. Consulte "Resumo da interrupção do serviço Amazon S3 na região norte da Virgínia (EUA-EAST-1)", <https://aws.amazon.com/message/41926>.



relevantes serem encaminhadas. A análise de post-mortem e a causa raiz detalhada do incidente serão atribuídas à equipe apropriada. Post-mortems são convocadas após qualquer problema operacional significativo, independentemente do impacto externo, e os documentos de Correction of Errors (COE – Correção de erros) são preparadas para que a causa raiz seja identificada e ações preventivas sejam adotadas no futuro. A implementação de medidas preventivas é acompanhada durante reuniões operacionais semanais.

Clientes podem alcançar e testar a resiliência na AWS

A AWS acredita que as instituições financeiras devem garantir que elas – e as funções econômicas críticas que executam – sejam resistentes a interrupções e falhas, qualquer que seja a causa. Interrupções prolongadas ou falhas definitivas podem causar perda de confiança nas instituições financeiras afetadas, além de causar perdas financeiras diretas devido ao não cumprimento de obrigações.

A AWS cria arquiteturas – e incentiva seus clientes a fazer o mesmo – considerando a ocorrência de falhas, a qualquer momento. Da mesma forma, como o Banco da Inglaterra reconhece, "queremos que as empresas planejem com a premissa de que qualquer parte de sua infraestrutura possa ser impactada, seja qual for o motivo".⁶ Ao projetar, criar e testar aplicações na AWS, os clientes podem alcançar seus objetivos de resiliência operacional. A AWS oferece os componentes base para qualquer tipo de cliente, de instituições financeiras a empresas de petróleo e gás e órgãos governamentais, para arquitetar aplicações que possam suportar eventos de grande escala. Nesta seção, debateremos como os clientes de instituições financeiras podem criar esse tipo de aplicação resiliente na Nuvem AWS.

Primeiros princípios

As equipes de campo da AWS, compostas por gerentes técnicos, arquitetos de soluções e especialistas em segurança, ajudam as instituições financeiras a criar aplicações de acordo com os objetivos de design, segurança e demais requisitos internos e regulatórios. Conforme refletido em nosso modelo de responsabilidade compartilhada, os clientes permanecem responsáveis por decidir como proteger seus dados e sistemas na Nuvem AWS, mas oferecemos guias para usuários, documentos de orientação e consultoria para auxiliar no processo. Antes de implantar uma aplicação de missão crítica, seja na Nuvem AWS ou em outro ambiente, instituições financeiras importantes passarão por extenso desenvolvimento e testes. Para um cliente que começa a criar uma aplicação na AWS com alta disponibilidade e resiliência em mente, recomendamos que ele responda a algumas perguntas fundamentais,⁷ que incluam, mas não se restrinjam a:

1. Quais problemas você está tentando resolver?
2. Quais aspectos da aplicação exigem níveis de disponibilidade específicos?
3. Quanto tempo de inatividade essa carga de trabalho (workload) pode realmente acumular em um ano?
4. Qual é o impacto real da indisponibilidade?

⁶ Charlotte Gerken, "The Bank of England's approach to operational resilience," (13 de junho de 2017), acessível em <https://www.bankofengland.co.uk/-/media/boe/files/speech/2017/the-boes-approach-to-operational-resilience.pdf>.

⁷ Recomendamos que os clientes analisem o [Cloud Adoption Framework](#) para desenvolver planos de adoção eficientes e eficazes. Consulte "Application Design for High Availability" sobre a determinação das necessidades de disponibilidade no whitepaper Pilar Confiabilidade da AWS: <https://d1.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf>.



As instituições financeiras e as concessionárias de mercado desempenham funções essenciais e não essenciais no setor de serviços financeiros. Desde a captação de depósitos até o processamento de empréstimos, a execução comercial e a liquidação de títulos, as entidades financeiras em todo o mundo prestam serviços cuja continuidade e resiliência são necessárias para garantir a confiança do público no sistema financeiro. Em todo o setor, para pagamentos, compensação, liquidação e outros tipos de aplicações importantes sistemicamente, os bancos centrais e os reguladores de mercado especificam um objetivo de tempo de recuperação (RTO - Recovery Time Objectives) discreto no padrão Principles for Financial Market Infrastructures (PFMI – Princípios para Infraestruturas do Mercado Financeiro): “O plano de [continuidade dos negócios] deve incorporar o uso de um site secundário e ser projetado para garantir que os sistemas críticos de tecnologia da informação (TI) possam retomar as operações dentro de duas horas após eventos perturbadores. O plano deve ser elaborado para permitir que as infraestruturas do mercado financeiro concluam a liquidação até o final do dia da interrupção, mesmo em circunstâncias extremas.”⁸

Além do RTO de duas horas, as agências reguladoras financeiras esperam que as entidades reguladas possam atender às RTOs e aos objetivos do ponto de recuperação (RPOs - Recovery Point Objectives) de acordo com a criticidade das aplicações, começando com a “aplicação de nível 1” como a mais crítica. Por exemplo, as entidades reguladas podem classificar seus RTOs e RPOs da seguinte maneira:

| Requisito de resiliência | Aplicação de nível 1 | Aplicação de nível 2 | Aplicação de nível 3 |
|----------------------------------|----------------------|----------------------|----------------------|
| Objetivo do tempo de recuperação | 2 horas | < 8 horas | 24 horas |
| Objetivo do ponto de recuperação | < 30 segundos | < 4 horas | 24 horas |

Embora as instituições financeiras relevantes sistemicamente possam ter mais de 8.000 a 10.000 aplicações, elas não classificam todas as aplicações de acordo com a mesma criticidade. Por exemplo, interrupções em uma aplicação para processar solicitações de empréstimos hipotecários são indesejáveis, mas uma instituição financeira que opera esse tipo de aplicação pode decidir tolerar uma RTO de 8 horas. Outros tipos de cargas de trabalho importantes, mas não necessariamente relevantes *sistemicamente*, incluem análise de mercado pós-negociação e chatbots voltados para atendimento ao cliente.

Embora a maioria das aplicações de entidades financeiras não seja crítica sob uma perspectiva sistêmica, a interrupção de algumas aplicações de Nível 1 comprometeria não apenas a segurança e a solidez da instituição financeira afetada, mas também de outras entidades do serviços financeiros e, possivelmente, a economia em geral. Por exemplo, uma aplicação de liquidação pode ser uma aplicação de Nível 1 e ter um RTO associado de 30 minutos e um RPO < 30 segundos. Essas aplicações são o coração dos mercados financeiros e as interrupções podem concretizar riscos operacionais, de liquidez e até mesmo de crédito. Para tais aplicações, há pouco ou praticamente nenhum tempo para alguém tomar uma decisão sobre como se recuperar de uma interrupção ou ativar o failover para um datacenter de backup. A recuperação precisaria ser automática e acionada com base em métricas e alarmes.⁹

⁸ Consideração essencial 17.6 dos PFMI, disponível em <https://www.bis.org/cpmi/publ/d101a.pdf>.

⁹ Os clientes podem ativar a recuperação automática usando uma variedade de serviços da AWS, incluindo métricas do [Amazon CloudWatch](#), [Amazon CloudWatch Events](#) e [AWS Lambda](#). Consulte também a seguinte apresentação da AWS re:Invent, “Recuperação de desastres e continuidade de negócios para instituições financeiras” para obter informações adicionais sobre os serviços aplicáveis da AWS e a arquitetura de exemplo: <https://www.youtube.com/watch?v=Xa-xTwhP1UU>.

A AWS fornece orientação aos clientes sobre as melhores práticas para a criação de aplicações resilientes e altamente disponíveis, inclusive por meio de nosso Well Architected Framework.¹⁰ Por exemplo, recomendamos que os componentes que compõem uma aplicação sejam independentes e isolados para fornecer redundância. Ao alterar componentes ou configurações em uma aplicação, os clientes devem garantir que eles possam reverter (roll back) quaisquer alterações caso a aplicação pareça não estar funcionando. Monitoramento e alarmes devem ser usados para acompanhar latência, taxas de erro e disponibilidade de cada solicitação, para todas as interdependências e para as principais operações do processo. Os dados coletados por meio do monitoramento devem permitir um diagnóstico eficiente dos problemas.¹¹ As melhores práticas para sistemas distribuídos devem ser implementadas para permitir a recuperação automatizada. Os processos de recuperação deve ser testado periodicamente – e com maior frequência aqueles complexos ou críticos.

Para instituições financeiras, pode ser difícil praticar esses princípios em ambientes tradicionais locais, muitos dos quais refletem décadas de consolidação com outras entidades e mudanças ad-hoc em suas infraestruturas de TI. Por outro lado, esses princípios são os que impulsionam o design da infraestrutura e dos serviços globais da AWS e formam a base de nossa orientação aos clientes sobre como obter a continuidade do serviço.¹² As instituições financeiras que usam os serviços da AWS podem aproveitar os serviços da AWS para melhorar sua resiliência, independentemente do estado de seus sistemas existentes.

Dos princípios de design à implementação

Os clientes precisam tomar muitas decisões: onde colocar seu conteúdo, onde executar as aplicações e como atingir níveis mais altos de disponibilidade e resiliência. Por exemplo, uma instituição financeira pode optar por executar sua aplicação de serviços bancários para dispositivos móveis em uma única região da AWS para aproveitar as várias zonas de disponibilidade, conforme descrito anteriormente e mostrado na Figura 2.

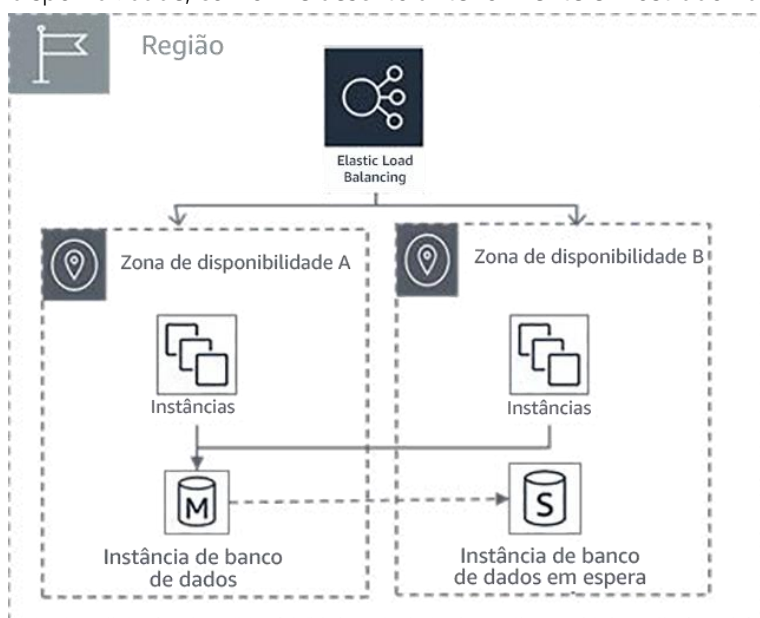


Figura 2. Exemplo de design Multi-AZ

Vamos dar o exemplo de uma implantação em duas AZs para ilustrar como AZs independentes proveem resiliência. Como mostra a Figura 2, o cliente implementa sua aplicação de internet banking de forma que sua arquitetura seja estável e consistente entre AZs. O cliente implementa sua aplicação de internet banking de forma que sua arquitetura seja estável e consistente entre AZs. O workload em cada AZ possui capacidade suficiente, assim como infraestrutura, configurações e políticas estáveis que mantêm ambas AZs atualizadas. O Elastic Load Balancer distribui o tráfego apenas para as instâncias íntegras. A camada de replicação de dados permite rápido failover no caso de uma instância de banco de dados falhar em uma das AZs, minimizando o tempo de inatividade do internet banking.

¹⁰ Consulte <https://aws.amazon.com/architecture/well-architected>.

¹¹ Uma variedade de serviços da AWS são compatíveis com essas práticas. Veja os exemplos nas páginas 26/28 em <https://d0.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf>.

¹² Para obter uma visão geral abrangente de nossas orientações aos clientes, consulte o whitepaper "Pilar Confiabilidade" (setembro de 2018) em <https://d0.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf>.



Comparados à infraestrutura e aos serviços da AWS, os ambientes tradicionais locais apresentam vários obstáculos para alcançar a resiliência operacional. Por exemplo, vamos supor que um evento significativo interrompa o funcionamento do datacenter primário de uma instituição financeira. A instituição financeira também tem um datacenter secundário, além de seu datacenter principal. A capacidade do datacenter secundário é capaz de lidar com apenas uma parcela da carga de trabalho geral que, de outra forma, operaria no datacenter primário (por exemplo, 11 mil servidores no centro secundário em vez de 12 mil servidores no centro primário; a capacidade da rede aumentou 300% no centro primário nos últimos quatro anos, mas apenas 250% no centro secundário) e erros na replicação apontam que os dados do centro secundário não foram atualizados nas últimas 36 horas. Além disso, fatores macroeconômicos aumentaram o volume de transações no datacenter primário em 15% nos últimos seis meses. Como resultado, a instituição financeira pode considerar que seu datacenter secundário não pode processar o volume atual de transações dentro de um determinado período, de acordo com seus requisitos internos e regulatórios.

Ao usar os serviços da AWS, a instituição financeira poderia aumentar a capacidade em intervalos frequentes para oferecer suporte a volumes crescentes de transações, além de acompanhar e gerenciar alterações para manter todas as implementações com as mesmas capacidades e arquiteturas atualizadas. Além disso, na AWS os clientes podem manter infraestrutura e backups inativos (cold) adicionais que podem ser ativados, se necessário, a um custo muito menor do que adquirir sua própria infraestrutura física. Esta não é uma questão hipotética. Os principais requisitos normativos destacam que as entidades reguladas devem levar em consideração a capacidade (recursos) para lidar com cenários adversos.¹³

Na AWS, os clientes também podem implantar workloads em AZs localizadas em várias regiões (Figura 3) para obter redundância de AZs e redundância de região. Os clientes que têm requisitos regulatórios, de armazenamento de dados em várias regiões ou desejam obter uma disponibilidade ainda maior, podem usar uma arquitetura multirregional. Em uma configuração multirregional, o cliente deve executar engenharia adicional para minimizar a perda de dados e garantir consistência de dados entre as regiões. Um componente de roteamento monitora o estado da aplicação, bem como as dependências. Essa camada de roteamento também gerencia failovers automáticos, alterando o destino quando um local não está íntegro e interrompendo temporariamente a replicação de dados. O tráfego irá apenas para regiões íntegras.

A AWS aprimora a resiliência operacional em comparação com os ambientes tradicionais locais, não apenas para failover, mas também para retornar à resiliência total. Para a instituição financeira com um datacenter secundário, pode ser necessário executar backup e restauração de dados por vários dias. Muitos ambientes tradicionais não apresentam replicação bidirecional, resultando em dados atuais no site de backup e em dados "desatualizados" no site primário, o que dificulta a obtenção de failback rápido. Na AWS, a instituição financeira não está "restritas", como estariam em um ambiente on-premises. A instituição financeira pode ativar (launch) rapidamente o workload em outro local. O ponto principal é que a infraestrutura e os serviços globais da AWS oferecem às instituições financeiras capacidade e performance para atender a objetivos agressivos de resiliência.

Para garantir a resiliência das aplicações, recomendamos que as instituições financeiras realizem testes contínuos de performance, carga e falha; usem amplamente registros, métricas e alarmes; mantenham manuais (runbooks) para relatar e acompanhar performance; além de validar a arquitetura por meio de testes reais e em grande escala, conhecidos como exercícios "game day". De acordo com os requisitos normativos de suas jurisdições, as instituições financeiras podem fornecer evidências de tais testes, manuais e exercícios às autoridades normativas financeiras.

¹³ Veja, por exemplo, a U.S. Securities and Exchange Commission (SEC), Regulation Systems Compliance and Integrity, 17 C.F.R. § 240, 242 e 249. Consulte também a adoção da versão: <https://www.sec.gov/rules/final/2014/34-73639.pdf>. Consulte também FFIEC, Business Continuity Planning, IT Examination Handbook (fevereiro de 2015), disponível em https://ithandbook.ffiec.gov/media/274725/ffiec_itbooklet_businesscontinuityplanning.pdf.

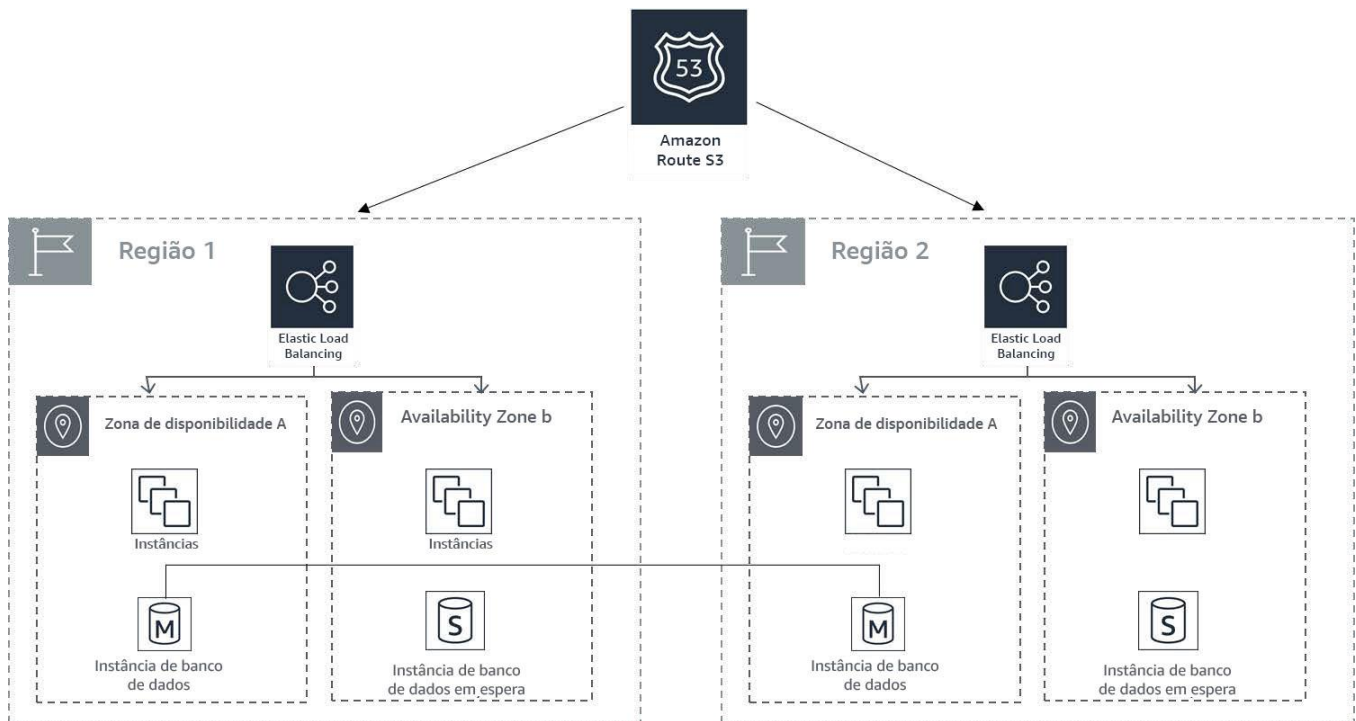


Figura 3. Exemplo de design multirregional

Mecanismos de garantia e conformidade

Estamos preparados para dar garantias sobre a abordagem da AWS para resiliência operacional e ajudar os clientes a obter confiança na segurança e a resiliência de seus workloads. Essa confiança pode ser obtida de várias maneiras, entre elas: relatórios sobre a infraestrutura e os serviços da AWS preparados por auditores independentes, além de serviços e ferramentas para monitorar, avaliar e testar seus ambientes na AWS, incluindo ainda a experiência direta com a AWS através de nossos recursos de auditoria.

Verificação independente de terceiros

Com nossa oferta padronizada e milhões de clientes ativos em praticamente todos os segmentos de negócios e setor público, fornecemos programas de conformidade para nosso ambiente de risco e controle, inclusive como lidamos com a resiliência operacional. A AWS opera milhares de controles que atendem aos mais altos padrões do setor. Para entender esses controles e como operá-los, os clientes podem acessar nosso relatório System and Organization Control (SOC – Controle de sistema e organização) 2 Tipo II, refletindo a verificação por meio de um auditor independente, que fornece uma visão geral do programa de resiliência da AWS. Além disso, um auditor independente validou o alinhamento da AWS com a norma ISO 27001. A International Organization for Standardization (ISO - Organização Internacional para Padronização) reúne especialistas para compartilhar conhecimento e desenvolver e publicar padrões internacionais uniformes que apoiam a inovação e fornecem soluções para os desafios globais. Além da ISO 27001, a AWS também se alinha às diretrizes da ISO 27017 sobre segurança da informação na nuvem e ao código de práticas ISO 27018 sobre proteção de dados pessoais na nuvem. A base desses padrões é o desenvolvimento e implementação de um rigoroso



programa de segurança. O Information Security Management System (ISMS – Sistema de gerenciamento de segurança da informação) exigido pela norma ISO 27001 define como a AWS gerencia a segurança de maneira holística e abrangente e inclui vários objetivos de controle (por exemplo, para os domínios A16 e A17) relevantes para a resiliência operacional. Com um Non-Disclosure Agreement (NDA – Contrato de não divulgação), os clientes podem fazer download desses relatórios e outros através do [AWS Artifact](#) – mais de 2.600 controles, padrões e requisitos de segurança no total. A AWS pode fornecer esses relatórios, às agências reguladoras mediante solicitação.

A AWS também [se alinha](#) com o National Institute of Standards and Technology (NIST – Instituto Nacional de Normas e Tecnologia) Cybersecurity Framework (CSF - Estrutura de segurança cibernética).

Desenvolvido originalmente para uso em entidades de infraestrutura críticas, o conjunto básico de disciplinas de segurança do CSF pode ser aplicado a qualquer organização e em qualquer setor, independentemente do tamanho. O U.S. Financial Services Sector Coordinating Council desenvolveu um Perfil de segurança cibernética específico para o setor de serviços financeiros (disponível [aqui](#)) que mapeia a CSF para uma variedade de normas e regulamentos internacionais, federais e estaduais dos EUA. O alinhamento da AWS com o CSF, atestado por um auditor terceiro, reflete a adequação dos serviços da AWS para aprimorar a segurança e a resiliência das entidades do setor financeiro.

Garantia direta para clientes

Os clientes também podem obter garantia contínua sobre a resiliência de suas próprias cargas de trabalho. Por meio de serviços e ferramentas disponíveis no console de gerenciamento da AWS, os clientes têm recursos de visibilidade, monitoramento e correção sem precedentes para garantir a segurança e a conformidade de seus próprios ambientes da AWS. As instituições financeiras não precisam mais contar com snapshots periódicos ou avaliações trimestrais e anuais para validar sua segurança e conformidade.

Considere apenas alguns exemplos das várias maneiras pelas quais os clientes obtêm garantia direta sobre a segurança e conformidade de seus recursos da AWS.¹⁴ Em primeiro lugar, os clientes podem integrar seus controles de auditoria a um sistema de notificação e fluxo de trabalho usando os serviços da AWS. Por exemplo, em um sistema desse tipo, uma alteração no estado de um servidor virtual de pendente para em execução resultaria em ações corretivas, criação de log e, conforme necessário, notificações à equipe apropriada. Os clientes também podem integrar seu sistema de notificação e fluxo de trabalho a um serviço de segurança cibernética oferecido pela AWS que utiliza tecnologia de machine learning, e detecta chamadas de API incomuns, implementações potencialmente não autorizadas entre outras atividades maliciosas.

Em segundo lugar, os clientes podem converter requisitos regulatórios em regras gerenciadas personalizadas e acompanhar continuamente alterações de configuração em seus recursos; por exemplo, se um banco exigir que os desenvolvedores não possam criar volumes de armazenamento não criptografados, o banco poderá definir uma regra de criptografia que identifique o volume fora de conformidade e o remova automaticamente.

Finalmente, e em terceiro lugar, outro serviço da AWS permite que aos clientes avaliem de forma automática a segurança de seu ambiente, analisando sua rede, sistema de arquivos e atividades de processo, coletando um amplo conjunto de dados das atividades e configurações. Esses dados incluem detalhes de comunicação com os serviços da AWS, uso de canais seguros, detalhes dos processos em execução, tráfego de rede entre os processos e muito mais, resultando em uma lista de descobertas (findings) e problemas de segurança ordenados por gravidade.

¹⁴ Os serviços da AWS discutidos nesta seção incluem: [Amazon CloudWatch Events](#), [AWS Config](#), [Amazon GuardDuty](#), [regras do AWS Config](#), e [Amazon Inspector](#).



Enquanto esses e outros serviços corrigem configurações não compatíveis ou vulnerabilidades de segurança, a AWS também recomenda que os clientes testem suas aplicações quanto à resiliência operacional. A instituição financeira deve testar as falhas transitórias nas dependências de suas aplicações (incluindo dependências externas), falhas em componentes e degradação em comunicações de rede. Um grande cliente desenvolveu software de [código aberto que](#) pode servir como base para esse tipo de teste. Para as preocupações de que agentes mal-intencionados possam acessar funções ou processos críticos, os clientes também podem realizar testes de penetração em seus ambientes da AWS.¹⁵

Por fim, os esforços da AWS para fornecer transparência sobre nosso ambiente de risco e controle não se restringem aos nossos relatórios de auditoria de terceiros ou em compromissos formais de auditoria. Nossa equipe de segurança e conformidade, arquitetos de soluções de segurança, engenheiros e equipes de campo se envolvem diariamente com clientes para resolver dúvidas e preocupações.

Essa interação pode ser através de ligação telefônica com a equipe de segurança da instituição financeira, uma reunião executiva com o diretor de segurança da informação (CISO) e CIO do cliente, uma reunião nos escritórios da AWS e inúmeras outras maneiras. Os clientes guiam nosso roadmap de infraestrutura e serviços, atender e exceder suas necessidades de segurança e resiliência é nosso objetivo número um.

¹⁵ Por exemplo, no Reino Unido, o Banco da Inglaterra desenvolveu a estrutura CBEST para testar a resiliência cibernética das empresas financeiras. Empresas de teste de penetração credenciadas tentam acessar ativos críticos da entidade-alvo. Uma empresa de inteligência de ameaças credenciada fornece inteligência de ameaças e orienta como os pentesters podem atacá-la. As instituições financeiras sujeitas à estrutura CBEST e que planejam realizar um teste de penetração em seus recursos na AWS precisam notificar a AWS enviando uma solicitação (em <https://aws.amazon.com/security/penetration-testing>) pois essa atividade pode ser detectada como violações de segurança proibidas e abuso de rede.