IBM Global Technology Services
Thought Leadership White Paper

Junho de 2015

Resiliência em Cloud

IBM

Sumário

Resumo executivo

No mundo de mobilidade e socialmente conectado como hoje, os usuários esperam estar conectados em todo lugar e sempre que desejarem, não importa o dispositivo e a localidade. Qualquer tolerância que havia para tempo de inatividade e perda de dados não existe mais considerando a velocidade de um mundo sempre conectado. Concentradas entre os dois extremos de soluções de recuperação de desastre de baixo custo e de replicação de alto custo, muitas organizações estão adotando modelos de cloud como uma forma mais acessível para atender aos requisitos para a rápida recuperação de sistemas e dados.

Cloud oferece um enorme potencial para reduzir os custos, aumentar a agilidade e reduzir riscos. Mas a falha em planejar adequadamente e implementar soluções de resiliência pode resultar em um aumento não intencional dos riscos da empresa. Muitos usuários de soluções em cloud assumem a existência de um nível de disponibilidade contínua que não é necessariamente provido em todos os serviços em cloud. Por outro lado, só porque o potencial de uma solução de resiliência melhor e mais ágil exista, não significa que a resiliência dos negócios esteja automaticamente garantida simplesmente porque uma carga de trabalho foi migrada para cloud. Quando se trata de resiliência, o modelo em cloud deve ser visto e avaliado como outro domínio de tecnologia— com requisitos funcionais e não funcionais de resiliência a serem definidos, avaliados, medidos e monitorados. As decisões corretas sobre cloud são críticas para as organizações reduzirem despesas e melhorarem a capacidade de responder a riscos, ameaças e oportunidades relacionados a cloud. No entanto, identificar requisitos, riscos, priorizá-los e alocar fundos para endereçá-los nem sempre é fácil. Para isso, as organizações precisam reunir e analisar as informações corretamente, para tomar decisões baseadas em valor e trabalhar com o gerenciamento de custos e riscos efetivos relacionados à resiliência.

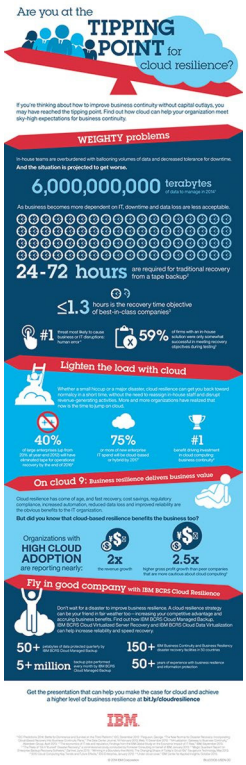
Seja migrando cargas de trabalho para plataformas baseadas em cloud ou seguindo um modelo de Recuperação de Desastre como Serviço (DRaaS), cloud requer uma mudança fundamental no que se refere ao gerenciamento de risco das empresas de forma integrada. Embora haja muita falta de planejamento de resiliência de negócios na maioria das implementações em cloud hoje, uma boa análise e planejamento podem ajudar as organizações a perceberem o enorme potencial que cloud oferece para melhoras a resiliência das empresas, com agilidade e encontrando o equilíbrio entre os requisitos de disponibilidade de serviços e a tolerância para risco.

O ponto de mudança da resiliência

Nos últimos anos, os ecossistemas de sistemas internos e externos usados para conduzir negócios diários eram mais restritos e o risco de exposição era muito menor. Em uma organização típica dos dias atuais, os usuários interagem com múltiplos sistemas, alavancando informações e serviços contidos interna e externamente para executar o trabalho. Conforme o número de sistemas, dados e usuários cresce— junto com a interdependência de análises e sistemas—o mesmo acontece com a complexidade e a necessidade de resiliência das empresas. Por exemplo, quando um pedido online é colocado, o sucesso dessa transação depende do website, da aplicação de e-commerce, do sistema de transação de back-office, do sistema que informa o warehouse o que escolher e para onde enviá-la e o sistema de inventário que atualiza o estoque no

warehouse. Se qualquer um desses ficar inativo, todo o processo será interrompido, incluindo os sistemas de relacionamento e sistemas que envolvem o acompanhamento da compra pelo cliente.

Sua empresa atingiu o ponto de mudança para a resiliência em cloud**? Veja o infográfico:**



O custo e o esforço de manter infraestruturas de resiliência levam muitas organizações que estão além de tecnologias de recuperação tradicionais de desastre para a resiliência em cloud. Com a capacidade para failover rápido, uma solução em cloud pode ajudar a assegurar a disponibilidade de aplicações e dados quase contínua, independentemente de quão geograficamente dispersos os sistemas e os usuários da organização possam estar. Cloud também pode trazer escalabilidade sem precedentes para a resiliência de negócios e a capacidade de fornecer rapidamente novos recursos de serviços que muitos provedores de resiliência comercial e de recuperação de desastre têm oferecido por muitos anos. A diferença é que cloud pode agora trazer alguns desses recursos sob o controle do cliente.

No entanto, até o momento, poucas aplicações foram projetadas para tirar o máximo de proveito dos recursos da resiliência em cloud. Grande parte do foco atual em projetos relacionados à cloud diz respeito a identificar e migrar cargas de trabalho de destino para cloud o mais rapidamente possível. Ferramentas de virtualização e todas as soluções em cloud não são inerentemente mais resistentes. Além disso, serviços específicos de cloud como corretagem, capacidade de orquestração e os sistemas de catálogo de serviços podem representar pontos críticos de falha que, se acontecerem, requerem paralisação de serviços para preservar dados e consistência transacional. Se a resiliência não for integrada na adoção inicial de cloud, as organizações estarão aceitando riscos, quer realizem isso ou não. Embora haja referências consistentes para alavancar cloud para recuperação de desastres, há pouca orientação sobre como usá-la de forma eficaz, incluindo testes para assegurar que a recuperação de desastre baseada em cloud e as estratégias de resiliência funcionarão como esperado.

Se as organizações não estiverem integrando a resiliência em sua adoção inicial de cloud, elas estarão aceitando os riscos, quer realizem isso ou não.

A realidade sobre a resiliência em cloud

Quando se trata de resiliência, a maioria das organizações tem dificuldade em responder algumas questões devido aos seus ambientes legados:

- Você pode quantificar de forma precisa o custo de uma hora de tempo de inatividade?
- Você pode fornecer evidência testada sobre o quão rapidamente é possível retomar as operações de negócios?
- Você sabe onde as suas concentrações de risco de rompimento de dados residem?
- Você sabe a extensão do impacto se algo acontecer?

Em média, uma falha de infraestrutura pode custar US$ 100.000 por hora e uma falha crítica de aplicação pode custar de US$ 500.000 a US$1 milhão por hora.[1]

Poucas organizações podem responder de forma confiável a essas perguntas para um ambiente em cloud. Implementações de cloud normalmente incluem padrões imprevisíveis de tráfego e de variações de larga escala esporádicas em volume de transações e capacidade devido a mudanças nos requisitos de negócios. Arquiteturas são mais abertas, com vários fornecedores, ISPs, sistemas de gerenciamento, opções de conexão e tecnologias. Com a mudança de tecnologias e padrões emergentes, cloud pode trazer aumento significativo em complexidade além de um nível de volatilidade que compõe ainda mais a complexidade. Conhecimento contínuo e monitoramento em tempo real do que é executado.

Com qualquer implementação, seja ela um modelo de Recuperação de Desastre como Serviço ou outra solução baseada em cloud, a complexidade e o impacto de indisponibilidades requerem envolvimento e a supervisão de especialistas de resiliência e a aplicação de métodos e técnicas formalizados com testes adequados. Por exemplo, mover o storage e processar a capacidade externamente ajuda a reduzir a concentração de risco e o impacto decorrente da indisponibilidade de um único site. No entanto, a mudança para outro site, sem planejamento e projeto cuidadosos em uma estratégia e arquitetura resiliente, pode resultar em um aumento do risco da organização em vez de reduzi-lo. As concentrações de risco, mesmo em implementações de vários sites, podem criar gargalos e falhas. E enquanto cloud assume acesso contínuo aos dados e à capacidade de cálculo, e a replicação desempenha um papel chave, isso também incorre no risco de replicar o dano.

A recuperação de sistemas em vários provedores e locais em cloud requer alta experiência e habilidade de integração de TI.

As organizações também precisam pensar sobre como integrar soluções em cloud de volta ao ambiente de produção legado. As cargas de trabalho baseadas em cloud das maiores empresas interagem com cargas de trabalho em execução em ambientes legados, o que significa que esta interoperabilidade deve ser levada em conta tanto para negócios no dia a dia quanto em situações de interrupção. Uma coordenação meticulosa e uma orquestração do novo ambiente híbrido são necessárias, especialmente quando se trata de testes relacionados com a resiliência e *failovers* de interrupção real, quando várias cargas de trabalho precisam ser deslocadas e ressincronizadas.

A sincronização é mais do que ter certeza de que a cópia secundária dos dados corresponda à primária e a automação é mais do que a programação de script do procedimento de reinicialização da aplicação.

A pressão regulamentar para as organizações provarem que podem continuar as operações usando sistemas de backup continua aumentando. Fornecer evidência de que a resposta sobre resiliência satisfaz as necessidades do negócio requer testes que efetivamente recriem a experiência do usuário, confirmando assim a eficácia e o valor do programa de resiliência. No passado, os reguladores ficaram principalmente interessados em systems of record. Hoje, nós vemos as expectativas para uma experiência sempre disponível, focada em sistemas de engajamento e resiliência crescente de negócios, visando permitir o processamento em tempo real para o marketing no local e a análise de dados não estruturados. As dependências de complexidade e interatividade entre estas famílias de processamento precisam ser incluídas nas estratégias e desenhos de plano de resiliência. Hoje, a reputação de toda organização é construída ou perdida através dos olhos do cliente em tempo real.

Testar em um ambiente em cloud traz o seu próprio conjunto de desafios. Por exemplo, o teste verdadeiro de recuperação de desastre exigirá isolar ambientes e caminhos de conexão desde então (você não pode ter os seus endereços IP de produção ativos em dois lugares ao mesmo tempo - no seu data center e na sua solução de resiliência em cloud).Isso significa descobrir como ter um segundo conjunto de endereços IP que são mascarados no ambiente de produção.Isso permitirá o teste abrangente sem contaminar a atividade de produção.

O gerenciamento e isolamento do endereço IP é mais crítico do que nunca em cloud. Obtê-lo errado pode expor a empresa a grandes riscos quando a Internet torna-se parte de seu processamento de produção e ambiente de teste de resiliência.

Em resumo, o escopo tradicional e estreito de validação e restauração de TI não é mais suficiente. Nem a execução de um ambiente de resiliência é a mesma que a execução de um ambiente de produção. A resiliência de cloud requer habilidades e experiência para assegurar que o design, arquitetura, orquestração, gerenciamento e monitoramento, relatório e controle certos estejam no local para fazê-la funcionar. Pode ser simples levantar um ambiente de recuperação de desastre em cloud, mas muito mais precisa ser feito em termos de recuperação de sistemas críticos de registro, de engajamento e de insight para fornecer prova de que a organização pode continuar a executar os negócios no caso de uma interrupção.

A abordagem correta para resiliência em cloud

A realidade de resiliência em cloud é que se você não projetá-la, implementá-la e mantê-la de forma correta, não a terá. Mas como uma organização se assegura de que está atuando corretamente desde o início? Boas práticas sugerem que fazer isso corretamente requer uma abordagem estruturada que permite que as organizações:

- Entendam a criticidade de serviços de negócios suportados por cargas de trabalho em cloud, negócios associados e requisitos de resiliência de TI e dependências de cloud/aplicações de legado/dados
- Identifiquem riscos relacionados e ações de mitigação
- Determinem estratégias de cloud mais apropriadas que atendam às necessidades de resiliência baseadas em negócios
- Documentem execuções de link, interdependências e pontos de sincronização entre ambientes de cloud e de legado
- Desenvolvam, implementem, testem e sustentem planos e procedimentos de negócios e de resiliência de TI
- Criem planos de validação e teste específicos de cloud e de cloud integrada ou de resiliência do legado
- Desenvolvam um roteiro de transição de cloud

Pode parecer muito difícil realizar o design e planejamento de uma infraestrutura de cloud resiliente, sem mencionar a implementação e o gerenciamento. No entanto, há algumas táticas chaves e etapas que as empresas podem seguir para planejar e gerenciar a resiliência em cloud. A Figura 1 descreve as quatro etapas da metodologia da IBM que considera a resiliência em cloud a partir da avaliação até o gerenciamento.

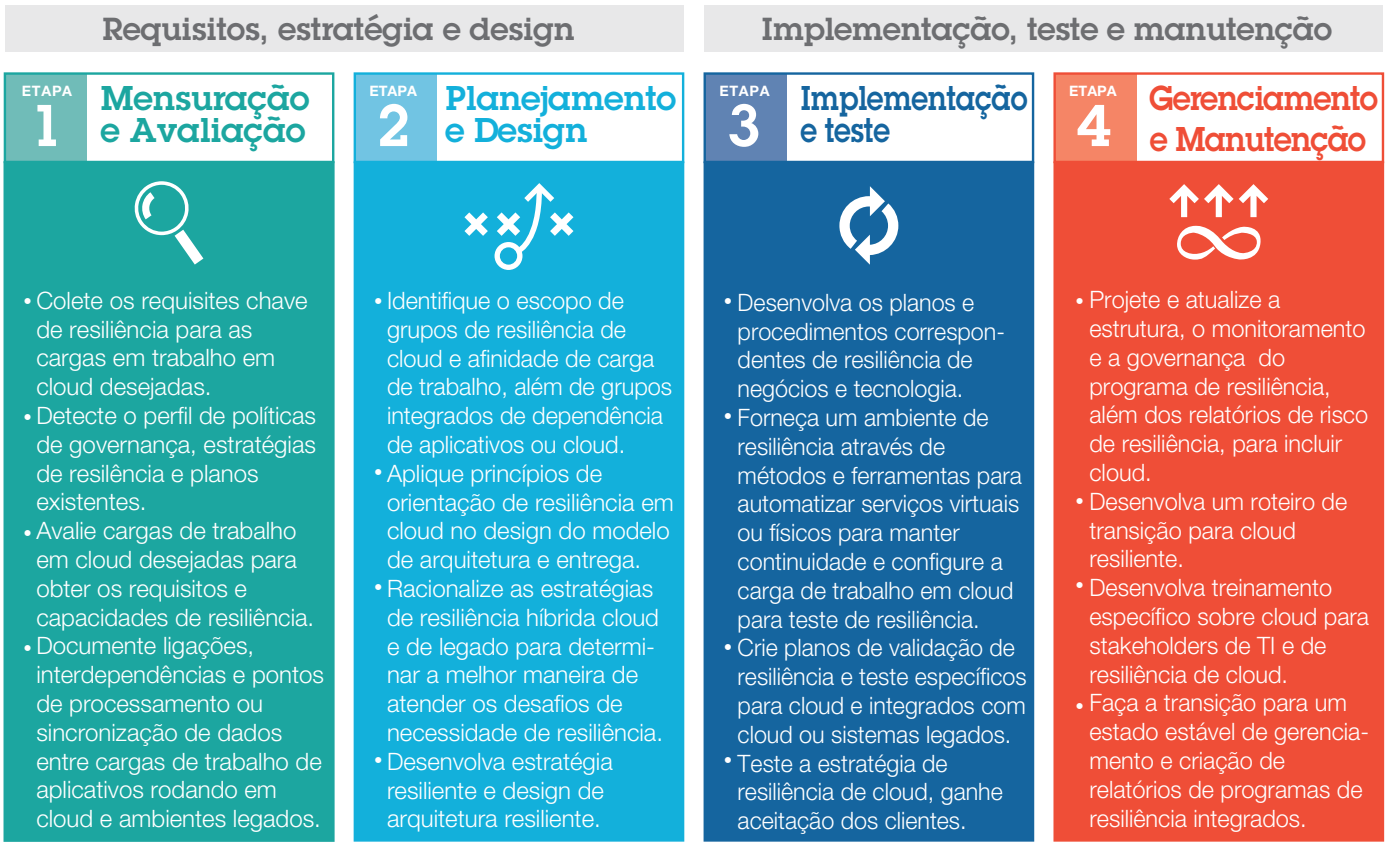


Figura 1. As quatro etapas da metodologia IBM.

Etapa 1 – Analisar e Avaliar

Poucas organizações, caso existam, podem dizer que possuem o seu ambiente de TI "sempre ativo e disponível". A resiliência da empresa deve estar sempre ligada ao valor do negócio. Uma abordagem estruturada pode ajudar as organizações a identificarem cuidadosamente os requisitos de negócios a partir da perspectiva de resiliência que conduzirá objetivos e métricas de resiliência (por ex., indicadores chave de desempenho e risco). É possível começar identificando e documentando camadas de resiliência e obtendo aprovação dos usuários corporativos sobre o tempo de recuperação, os objetivos do ponto de recuperação para cada camada e quais funções de negócios serão mapeadas para quais camadas. Isso lhe dará algumas medidas para usar ao avaliar diferentes recursos e funções de cloud.

Com essas informações, as organizações precisam estar aptas para entenderem as interdependências dos serviços e da infraestrutura e o impacto que elas têm nesses objetivos de negócios. Após você entender os riscos, é possível desenvolver

uma estratégia e arquitetura de resiliência apropriada que não apenas atenda às necessidades de negócios, mas que permita que você prove isso. Atividades chave nesse processo incluem:

- Coletar requisitos chave de resiliência de negócios para cargas de trabalho em cloud
- Geração de perfis de cadeias de aplicações existentes com componentes de infraestrutura e dados, políticas aplicáveis, estratégias e planos de resiliência associados
- Avaliar cargas de trabalho em cloud no que diz respeito a requisitos e recursos de resiliência
- Documentar execuções de link, interdependências e pontos de sincronização de processamento/dados entre cargas de trabalho de aplicações em execução em cloud ou em ambientes de TI de legado

As organizações não podem se dar ao luxo de ter todo o seu ambiente de TI ativo o tempo inteiro." A resiliência precisa ser vinculada a valor de negócio.

Etapa 2 – Planejar e Projetar

O design de cloud deve considerar a maneira completamente integrada na qual as organizações "operam o negócio", incluindo dependências de serviço. No entanto, altos níveis de abstração em cloud podem criar desafios na identificação e na documentação de projetos de dependência de serviço. É aí que a Arquitetura de Cloud pode ajudar com conjuntos de ferramentas de gerenciamento que incluem provisionamento, replicação, automação, monitoramento e relatórios.

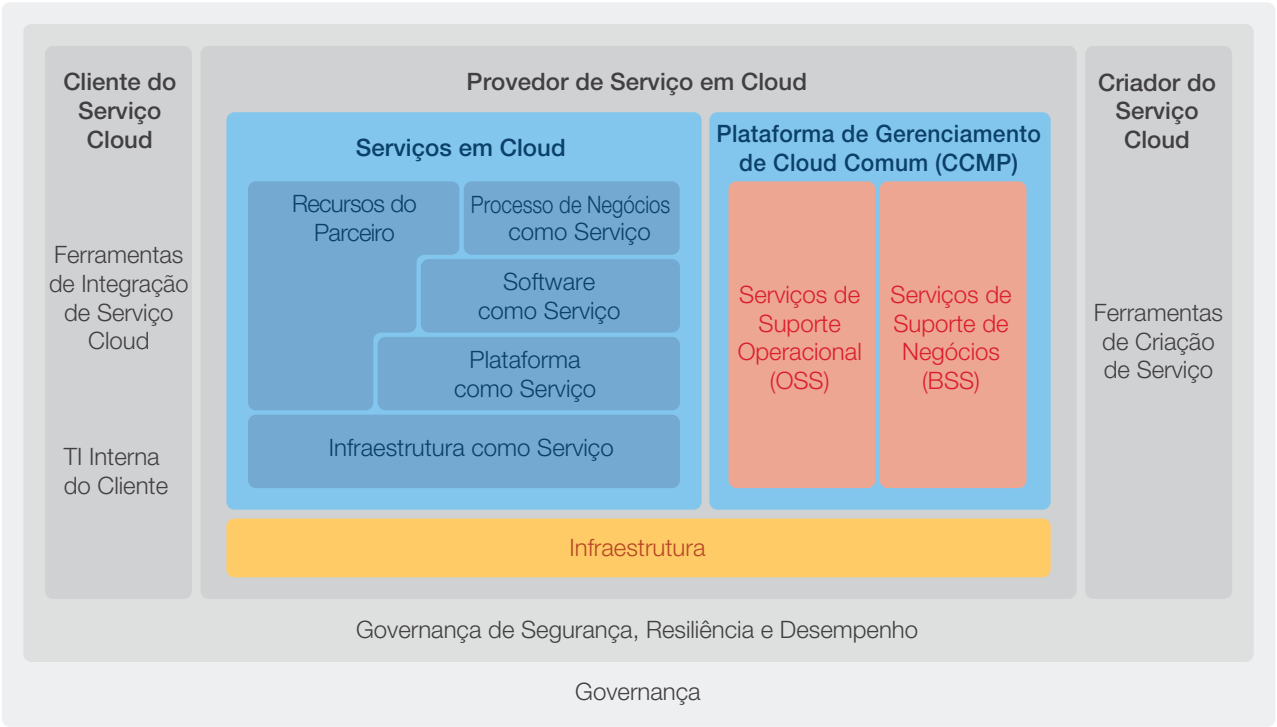


Figura 2. A Arquitetura de Cloud pode ajudar a identificar interdependências.

Para ajudar a alavancar essas ferramentas efetivamente, é possível combinar a arquitetura com a metodologia do Plano de Resiliência da IBM para fornecer um entendimento claro de interdependências de nível de aplicações, encerrar e reiniciar a sequência bem como o processamento e pontos de sincronização de dados para cargas de trabalho através de ambientes de TI em cloud e tradicionais. Níveis de concentração de risco também devem ser documentados seja devido a gargalos de capacidade ou a pontos de falha.

A metodologia do Plano de Resiliência pode ajudá-lo a entender se sua empresa possui um risco que seja aceitável ou que deseja evitar e minimizar. Em outras palavras, você pode optar por não fazer nada sobre um risco ou pode melhorar a sua infraestrutura para ajudar a assegurar que poderá lidar com os eventos se eles ocorram. Apenas quando o conjunto completo de requisitos funcionais e não funcionais (incluindo resiliência) forem entendidos, as organizações podem ir para a fase de planejamento e design, que inclui:

- Identificar requisitos de resiliência no escopo para cargas de trabalho e grupos de dependência de cloud/aplicações legado
- Entender o impacto de fornecer tempo de espera sobre tempo de recuperação e objetivos de ponto de recuperação
- Aplicar princípios de direcionamento de resiliência em cloud no design da arquitetura e do modelo de entrega
- Racionalizar estratégias de legado e de resiliência híbrida em cloud para determinar a melhor solução para atender às necessidades de disponibilidade
- Desenvolver estratégia e design de arquitetura resilientes

Etapa 3 – Implementar e Testar

Percepções falsas sobre cloud têm perpetuado a ideia de que o teste é simplesmente uma questão de provisionamento do que você precisa executar o teste e, em seguida, retirar o provisionamento para voltar para onde você estava. Criar e projetar corretamente um ambiente de teste exige muito mais do que simplesmente ativar uma infraestrutura ou fazer uma cópia dos dados sobre a cloud. As organizações precisam ser capazes de manter rigoroso gerenciamento de endereços IP, limites de jurisdição sobre cópias de dados e uma trilha de evidência de que elas não só executaram o teste, mas podem produzir resultados esperados a resultados reais.

Antes da implementação e teste, você precisará pensar sobre os resultados finais: o teste deve ser realista e ser capaz de "administrar os negócios" em um ambiente alternativo quando ocorrer uma grande interrupção de serviço. Com essas informações, é possível desenvolver planos e procedimentos de negócios e de resiliência de TI correspondentes:

- Fazendo provisão de ambiente de resiliência, usando métodos e ferramentas para automatizar servidores virtuais ou físicos para continuidade e configurar a carga de trabalho de cloud para teste de resiliência
- Criando planos de validação e teste específicos de cloud e de cloud integrada ou de resiliência do legado (podem incluir a introdução regular de falhas planejadas para testar resiliência de componente/serviço em tempo real)
- Testando a estratégia de resiliência em cloud e ganhando aceitação do cliente
- Retendo evidência de escopo de teste e resultados para propósitos de auditoria e relatório

O teste parcial ou em nível de componente combinado com a "crença de que as situações irão se resolver sozinhas" no momento da interrupção não é mais aceitável.

Etapa 4 – Gerenciar e Sustentar

A velocidade e flexibilidade da cloud pode trazer grande agilidade aos usuários, mas isso também é frequentemente acompanhado por um alto grau de volatilidade. Controle robusto, processos de gerenciamento e controle são necessários para manter recursos de resiliência sincronizados com o ambiente de produção. Monitoramento e relatório são importantes, pois resiliência não é um projeto "uma vez feito está concluído". Em vez disso, ela é um processo operacional e os executivos precisam saber o estado atual da empresa a qualquer momento— e especialmente no caso de uma indisponibilidade não planejada. Etapas para gerenciar e sustentar recursos de resiliência incluem:

- Design/atualização da estrutura de programa de resiliência, monitoramento, controle e relatório de risco de resiliência para incluir cloud
- Desenvolvimento de roteiro de transição em cloud resiliente
- Desenvolvimento de educação específica de cloud para investidores em resiliência de TI/Cloud
- Execução da transição para gerenciamento e relatório do plano de resiliência
- Manutenção de verificações e saldos apropriados para:
  - Garantia (incluindo terceiros) e evidência
  - Disponibilidade das aplicações
  - Disponibilidade do processo, estabilidade e reputação do fornecedor, mobilidade para migrar para um outro local/fornecedor
  - Requisitos de continuidade
  - Rede
  - Local, proteção, segregação de dados
  - Governança, risco e conformidade (GRC)

Conclusão

Em um mundo sempre conectado, a complexidade e o impacto de indisponibilidades requer mais atenção para as soluções de design e de gerenciamento da resiliência dos negócios.

A resiliência baseada em serviço e sistemas complexos de vários provedores demonstra que você precisa pensar diferente. A evolução de cloud trouxe expectativas de eficiências e economias significativas para recuperação de desastre que não foram realizadas em grande escala. Hoje, ainda há poucas soluções de resiliência em cloud projetadas, implementadas e testadas adequadamente.

A realidade é que a combinação de ambientes de TI tradicionais e baseados em cloud não vai desaparecer tão cedo, nem os recursos de cloud de recuperação de desastre "integrados" assumidos simplificam a resiliência — de fato, eles a tornam mais complexa. O risco pode ser significativamente aumentado quando as organizações adquirem e implementam soluções de cloud sem o envolvimento e a supervisão de especialistas de resiliência, e não aplicam métodos e técnicas formalizados com testes adequados.

A partir de serviços em cloud e soluções de resiliência de aplicações de grande escala, a IBM tem a experiência, conhecimento e tecnologia comprovados para ajudar sua empresa com uma resiliência integrada, face às ameaças, em qualquer ambiente de TI, incluindo cloud pública, privada ou híbrida.

Aprenda mais sobre como a metodologia de resiliência de quatro fases foi aplicada no desenvolvimento de disponibilidade contínua usando cloud:

A sua jornada para estar sempre disponível em quatro etapas

Os nossos serviços de resiliência de negócios podem ajudá-lo a planejar e projetar para a implementação e o gerenciamento de resiliência em cloud, com um forte compromisso com a compreensão de requisitos de negócios em constante mudança.

Para mais informações

Para aprender mais sobre os Serviços de Resiliência IBM, entre em contato com o representante da IBM ou o Parceiro de Negócios IBM ou visite o seguinte website: **ibm.com**/services/continuity

Adicionalmente, o Banco IBM pode ajudá-lo a adquirir as soluções de TI que os seus negócios precisam. Para clientes qualificados para crédito, nós podemos customizar uma solução de financiamento de TI para atender aos seus requisitos de negócios, permitir gerenciamento de caixa eficaz e melhorar o custo total de sua propriedade. O Banco IBM é a sua opção mais inteligente para financiar investimentos de TI críticos e impulsionar os seus negócios. Para obter mais informações, visite: ibm.com/financing: **ibm.com**/financing

IBM Global Technology Services
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América,
em junho de 2015

[1] IDC, "DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified." Stephen Elliot. Dezembro de 2014, IDC #253155.

Recicle

BUW03048-USEN-00