

Pilar Excelência operacional



Pilar Excelência operacional: AWS Well-Architected Framework

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Resumo e introdução	1
Introdução	1
Excelência operacional	3
Princípios de design	3
Definição	4
Organização	6
Prioridades da organização	6
OPS01-BP01 Avaliar as necessidades dos clientes externos	6
OPS01-BP02 Avalie as necessidades dos clientes internos	8
OPS01-BP03 Avaliar os requisitos de governança	9
OPS01-BP04 Avaliar os requisitos de conformidade	12
OPS01-BP05 Avaliar o cenário de ameaças	15
OPS01-BP06 Avalie as compensações	17
OPS01-BP07 Gerenciar os benefícios e os riscos	19
Modelo operacional	20
Representações do modelo operacional 2 por 2	21
Relacionamentos e propriedade	31
Cultura organizacional	42
OPS03-BP01 Patrocínio executivo	42
OPS03-BP02 Os membros da equipe estão capacitados para executar ações quando os resultados estão em risco.	43
OPS03-BP03 Incentivo ao escalonamento	44
OPS03-BP04 Comunicações oportunas, claras e acionáveis	45
OPS03-BP05 Incentivo à experimentação	48
OPS03-BP06 Os membros da equipe estão capacitados e são incentivados a manter e a aumentar seus conjuntos de habilidades.	51
OPS03-BP07 Fornecer recursos adequados às equipes	53
OPS03-BP08 Opiniões diversas são incentivadas e procuradas dentro e entre equipes	53
Preparar	55
Implementar a observabilidade	55
OPS04-BP01 Identificar os indicadores-chave de performance	56
OPS04-BP02 Implementar a telemetria de aplicações	58
OPS04-BP03 Implementar a telemetria da experiência do usuário	61
OPS04-BP04 Implementar a telemetria de dependências	64

OPS04-BP05 Implementar rastreamento distribuído	67
Design das operações	69
OPS05-BP01 Usar o controle de versão	70
OPS05-BP02 Testar e valide as alterações	71
OPS05-BP03 Usar sistemas de gerenciamento de configuração	75
OPS05-BP04 Usar sistemas de gerenciamento de compilação e de implantação	78
OPS05-BP05 Executar o gerenciamento de patches	80
OPS05-BP06 Compartilhar os padrões de design	83
OPS05-BP07 Implementar práticas para aprimorar a qualidade do código	86
OPS05-BP08 Usar vários ambientes	89
OPS05-BP09 Fazer alterações frequentes, pequenas e reversíveis	90
OPS05-BP10 Automatizar totalmente a integração e a implantação	92
Mitigar riscos de implantação	93
OPS06-BP01 Preparar-se para alterações malsucedidas	94
OPS06-BP02 Testar as implantações	96
OPS06-BP03 Utilizar estratégias de implantação seguras	99
OPS06-BP04 Automatizar os testes e a reversão	103
Prontidão operacional e gerenciamento de alterações	107
OPS07-BP01 Garantir a capacidade da equipe	107
OPS07-BP02: Garantir uma análise consistente da prontidão operacional	109
OPS07-BP03 Usar runbooks para realizar procedimentos	113
OPS07-BP04 Usar manuais para investigar problemas	117
OPS07-BP05 Tomar decisões embasadas para implantar sistemas e alterações	122
OPS07-BP06 Viabilizar planos de suporte para workloads de produção	124
Operar	128
Utilizar a observabilidade da workload	128
OPS08-BP01 Analisar métricas de workload	129
OPS08-BP02 Analisar logs de workloads	131
OPS08-BP03 Analisar rastreamentos de workload	134
OPS08-BP04 Criar alertas acionáveis	136
OPS08-BP05 Criar painéis	139
Compreensão da integridade operacional	142
OPS09-BP01 Medir metas operacionais e KPIs com métricas	143
OPS09-BP02 Comunicar o status e as tendências para garantir a visibilidade da operação	144
OPS09-BP03 Revisar as métricas operacionais e priorizar a melhoria	146

Resposta a eventos	148
OPS10-BP01 Usar um processo para gerenciamento de eventos, incidentes e problemas ..	149
OPS10-BP02 Ter um processo por alerta	154
OPS10-BP03 Priorizar eventos operacionais com base no impacto nos negócios	155
OPS10-BP04 Definir caminhos para escaladas	156
OPS10-BP05 Definir um plano de comunicação com o cliente para interrupções	157
OPS10-BP06 Comunicar o status por meio de painéis	162
OPS10-BP07 Automatizar respostas a eventos	163
Evoluir	166
Aprenda, compartilhe e aprimore	166
OPS11-BP01 Ter um processo para a melhoria contínua	167
OPS11-BP02 Executar análise pós-incidente	169
OPS11-BP03 Implementar loops de feedback	170
OPS11-BP04 Realizar o gerenciamento de conhecimento	173
OPS11-BP05 Definir motivadores de melhoria	176
OPS11-BP06 Validar insights	178
OPS11-BP07 Fazer análises das métricas de operações	179
OPS11-BP08 Documentar e compartilhar as lições aprendidas	180
OPS11-BP09 Alocar tempo para fazer melhorias	182
Conclusão	184
Colaboradores	185
Leitura adicional	186
Revisões do documento	187

Pilar Excelência operacional: AWS Well-Architected Framework

Data de publicação: 3 de outubro de 2023 ([Revisões do documento](#))

O foco deste artigo é o pilar Excelência operacional do AWS Well-Architected Framework. Ele fornece orientações para ajudar você a aplicar as práticas recomendadas em design, entrega e manutenção das workloads da AWS.

Introdução

O [AWS Well-Architected Framework](#) ajuda você a entender os benefícios e os riscos das decisões que você toma ao criar workloads na AWS. Ao usar o Framework, você aprenderá as práticas operacionais e de arquitetura recomendadas para projetar e operar workloads confiáveis, seguras, eficientes, econômicas e sustentáveis na nuvem. Ele permite avaliar com consistência as operações e arquiteturas em relação às práticas recomendadas e identificar áreas de melhoria. Acreditamos que ter workloads do Well-Architected projetadas com as operações em mente aumenta significativamente a probabilidade de êxito nos negócios.

A estrutura é baseada em seis pilares:

- Excelência Operacional
- Segurança
- Confiabilidade
- Eficiência de performance
- Otimização de custos
- Sustentabilidade

Este documento enfoca o pilar de excelência operacional e como aplicá-lo como base de suas soluções do Well-Architected. É difícil alcançar excelência operacional em ambientes em que as operações são percebidas como uma função isolada e distinta das linhas de equipes de negócios e desenvolvimento para as quais elas oferecem suporte. Ao adotar as práticas deste documento, você poderá criar arquiteturas que fornecem informações sobre seu status, que são ativadas para operação eficaz/eficiente e resposta a eventos, e podem continuar a melhorar e apoiar seus objetivos de negócios.

Este documento é destinado a pessoas que ocupam cargos de tecnologia, como diretores de tecnologia (CTOs), arquitetos, desenvolvedores e membros da equipe de operações. Depois de ler este documento, você entenderá as melhores práticas e estratégias da AWS a serem usadas ao projetar arquiteturas de nuvem para excelência operacional. Este documento não fornece detalhes de implementação ou padrões de arquitetura. No entanto, ele inclui referências a recursos apropriados para essas informações.

Excelência operacional

Na Amazon, definimos a excelência operacional como um compromisso com a construção correta de software, ao mesmo tempo em que oferecemos uma ótima experiência do cliente. Ela contém as práticas recomendadas para organizar sua equipe, projetar sua workload, operar em escala e evoluir ao longo do tempo. A excelência operacional ajuda a sua equipe a se concentrar por mais tempo na criação de novos recursos que beneficiem os clientes e menos tempo em manutenção e combate a problemas. Para construir corretamente, buscamos as práticas recomendadas que resultam em sistemas bem executados, uma workload equilibrada para você e sua equipe e, o mais importante, uma ótima experiência do cliente.

O objetivo da excelência operacional é colocar novos recursos e correções de bugs nas mãos dos clientes de maneira rápida e confiável. As organizações que investem em excelência operacional sempre encantam os clientes à medida que criam novos recursos, fazem alterações e lidam com falhas. Ao longo do caminho, a excelência operacional leva à integração contínua e entrega contínua (CI/CD) ao ajudar os desenvolvedores a alcançar resultados de alta qualidade de forma consistente.

Princípios de design

Os cinco princípios de design para excelência operacional na nuvem são:

- **Execute operações como código:** Na nuvem, você pode aplicar a mesma disciplina de engenharia usada para o código da aplicação em todo o ambiente. É possível definir toda a sua workload (aplicações, infraestrutura etc.) como código e atualizá-la com código. Você pode criar um script dos seus procedimentos de operações e automatizar o processo acionando-o em resposta a eventos. Ao executar operações como código, você limita o erro humano e cria respostas consistentes aos eventos.
- **Fazer alterações frequentes, pequenas e reversíveis:** projete workloads escaláveis e com acoplamento fraco para permitir que os componentes sejam atualizados regularmente. Técnicas de implantação automatizadas, bem como mudanças menores e incrementais, reduzem o raio de expansão e permitem uma reversão mais rápida se ocorrerem falhas. Isso aumenta a confiança na entrega de mudanças benéficas à workload, mantendo a qualidade e possibilitando uma rápida adaptação às mudanças nas condições do mercado.
- **Refine os procedimentos operacionais regularmente:** À medida que você evolui as workloads, desenvolva as operações de forma adequada. ao usar os procedimentos de operação, procure oportunidades para melhorá-los. Organize análises regularmente e valide se todos os

procedimentos estão em vigor e se as equipes estão familiarizadas com eles. Ao identificar lacunas, atualize os procedimentos adequadamente. Comunique as atualizações dos procedimentos a todas as partes interessadas e equipes. Promova o aprendizado gamificado em suas operações para compartilhar as práticas recomendadas e instruir as equipes.

- Preveja falhas: Execute os exercícios “pré-mortem” para identificar as potenciais origens de falhas, para que assim elas possam ser removidas ou mitigadas. Teste cenários de fala e valide como você compreende o impacto deles. Teste os procedimentos de resposta para garantir que sejam eficazes e que as equipes estejam familiarizadas com o processo. Organize dias de jogo periódicos para testar workloads da equipe a eventos simulados.
- Aprenda com todas as falhas operacionais: Promova a melhoria com as lições aprendidas em todos os eventos e falhas operacionais. Compartilhe o que foi aprendido com as equipes e a organização inteira.
- Usar serviços gerenciados: reduza a carga operacional usando serviços gerenciados da AWS sempre que possível. Crie procedimentos operacionais em torno das interações com esses serviços.
- Implementar a observabilidade para obter insights acionáveis: obtenha uma compreensão abrangente do comportamento, da performance, da confiabilidade, do custo e da integridade da workload. Estabeleça indicadores-chave de desempenho (KPIs) e aproveite a telemetria de observabilidade para tomar decisões fundamentadas e agir imediatamente quando os resultados obtidos estiverem em risco. Melhore proativamente o desempenho, a confiabilidade e o custo com base em dados de observabilidade úteis.

Definição

Existem quatro áreas de práticas recomendadas para excelência operacional na nuvem:

- Organizar
- Preparar
- Operar
- Evoluir

A liderança da sua organização define objetivos empresariais. Sua organização deve compreender requisitos e prioridades e usá-los para organizar e conduzir trabalhos para apoiar a obtenção de resultados empresariais. Sua workload deve emitir as informações necessárias para apoiá-la. A implementação de serviços para ativar a integração, a implantação e a entrega de sua workload

criará um fluxo maior de alterações benéficas na produção por meio da automação de processos repetitivos.

Pode haver riscos inerentes à operação da workload. Você deve compreender esses riscos e tomar uma decisão embasada para entrar na produção. Suas equipes devem ser capazes de dar suporte à sua workload. As métricas operacionais e de negócios derivadas dos resultados de negócios desejados ajudarão você a compreender a integridade da workload e das atividades de operações, bem como responder a incidentes. Suas prioridades mudarão à medida que suas necessidades de negócios e o ambiente de negócios mudarem. Use isso como um ciclo de comentários para promover continuamente melhorias para a sua organização e a operação da sua workload.

Organização

Você precisa entender as prioridades da sua organização, a estrutura organizacional e como ela oferece suporte aos membros da equipe, para que eles possam ajudar nos resultados da empresa.

Para capacitar a excelência operacional, você deve compreender o seguinte:

Tópicos

- [Prioridades da organização](#)
- [Modelo operacional](#)
- [Cultura organizacional](#)

Prioridades da organização

Suas equipes precisam ter um entendimento compartilhado de toda a sua carga de trabalho, da função que desempenham em tudo isso e dos objetivos de negócios compartilhados a fim de definir as prioridades que permitirão o êxito dos negócios. Prioridades bem definidas maximizarão os benefícios dos seus esforços. Analise suas prioridades regularmente para que elas possam ser atualizadas à medida que as necessidades da sua organização mudarem.

Práticas recomendadas

- [OPS01-BP01 Avaliar as necessidades dos clientes externos](#)
- [OPS01-BP02 Avalie as necessidades dos clientes internos](#)
- [OPS01-BP03 Avaliar os requisitos de governança](#)
- [OPS01-BP04 Avaliar os requisitos de conformidade](#)
- [OPS01-BP05 Avaliar o cenário de ameaças](#)
- [OPS01-BP06 Avalie as compensações](#)
- [OPS01-BP07 Gerenciar os benefícios e os riscos](#)

OPS01-BP01 Avaliar as necessidades dos clientes externos

Envolva as principais partes interessadas, incluindo equipes corporativas, de desenvolvimento e operacionais, a fim de determinar onde concentrar os esforços nas necessidades de clientes

externos. Isso garantirá que você tenha um entendimento completo do suporte às operações necessário para obter os resultados desejados nos negócios.

Antipadrões comuns:

- Você decidiu não ter suporte ao cliente fora do horário comercial principal, mas não analisou dados históricos de solicitação de suporte. Você não sabe se isso afetará seus clientes.
- Você está desenvolvendo um novo recurso, mas não envolveu seus clientes para descobrir se ele é desejado, em qual formato é desejado e sem experimentação para validar a necessidade e o método de entrega.

Benefícios do estabelecimento desta prática recomendada: Os clientes cujas necessidades estão atendidas têm muito mais probabilidade de permanecerem como clientes. Avaliar e compreender as necessidades de clientes externos informará como você priorizará seus esforços para entregar valor empresarial.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Alto

Orientações para a implementação

- Compreender as necessidades empresariais: o sucesso nos negócios é possibilitado pelos objetivos e pelo entendimento compartilhados entre as partes interessadas, incluindo equipes corporativas, de desenvolvimento e de operações.
 - Analisar os objetivos, as necessidades e as prioridades empresariais dos clientes externos: envolva as principais partes interessadas, incluindo as equipes corporativas, de desenvolvimento e de operações, para discutir as metas, as necessidades e as prioridades dos clientes externos. Isso garantirá que você tenha um entendimento completo do suporte às operações que é necessário para obter resultados nos negócios.
 - Estabelecer uma compreensão compartilhada: estabeleça uma compreensão compartilhada das funções corporativas sobre a workload, as funções de cada uma das equipes na operação da workload e de como esses fatores oferecem apoio aos seus objetivos empresariais compartilhados entre os clientes internos e externos.

Recursos

Documentos relacionados:

- [AWS Well-Architected Framework Concepts – Feedback loop \(Conceitos do AWS Well-Architected Framework: loop de feedback\)](#)

OPS01-BP02 Avalie as necessidades dos clientes internos

Envolva as principais partes interessadas, incluindo equipes corporativas, de desenvolvimento e operacionais, ao determinar onde concentrar os esforços nas necessidades de clientes internos. Isso garantirá que você tenha um entendimento completo do suporte às operações necessário para obter resultados nos negócios.

Use suas prioridades estabelecidas para concentrar seus esforços de melhoria onde eles terão maior impacto (por exemplo, desenvolvendo habilidades de equipe, melhorando a performance da carga de trabalho, reduzindo custos, automatizando runbooks ou aprimorando o monitoramento). Atualize suas prioridades conforme as necessidades mudam.

Antipadrões comuns:

- Você decidiu alterar as alocações de endereços IP para suas equipes de produtos, sem consultá-las, para facilitar o gerenciamento da sua rede. Você não sabe o impacto que isso terá em suas equipes de produtos.
- Você está implementando uma nova ferramenta de desenvolvimento, mas não envolveu seus clientes internos para descobrir se ela é necessária ou se é compatível com as práticas que eles realizam.
- Você está implementando um novo sistema de monitoramento, mas não entrou em contato com seus clientes internos para descobrir se eles têm necessidades de monitoramento ou relatórios que devam ser consideradas.

Benefícios do estabelecimento desta prática recomendada: Avaliar e compreender as necessidades de clientes internos informará como você priorizará seus esforços para entregar valor empresarial.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Alto

Orientações para a implementação

- Compreenda as necessidades empresariais: o sucesso nos negócios é possibilitado pelos objetivos e pelo entendimento compartilhados entre as partes interessadas, incluindo equipes corporativas, de desenvolvimento e de operações.

- Analise os objetivos, as necessidades e as prioridades empresariais dos clientes internos: envolva as principais partes interessadas, incluindo as equipes corporativas, de desenvolvimento e de operações, para discutir as metas, as necessidades e as prioridades dos clientes internos. Isso garantirá que você tenha um entendimento completo do suporte às operações que é necessário para obter resultados nos negócios.
- Estabeleça uma compreensão compartilhada: estabeleça um entendimento compartilhado das funções corporativas sobre a workload, as funções de cada uma das equipes na operação da workload e de como esses fatores apoiam seus objetivos empresariais compartilhados entre os clientes internos e externos.

Recursos

Documentos relacionados:

- [AWS Well-Architected Framework Concepts – Feedback loop \(Conceitos do AWS Well-Architected Framework: loop de feedback\)](#)

OPS01-BP03 Avaliar os requisitos de governança

Governança refere-se a um conjunto de políticas, regras ou frameworks que uma empresa usa para atingir metas de negócios. Os requisitos de governança são gerados dentro da organização. Eles podem afetar os tipos de tecnologia que você escolhe ou influenciar a maneira como você opera sua workload. Incorpore requisitos de governança organizacional em sua workload. Conformidade é a capacidade de demonstrar que você implementou os requisitos de governança.

Resultado desejado:

- Os requisitos de governança são incorporados ao design arquitetural e à operação da workload.
- Você pode fornecer prova de que seguiu os requisitos de governança.
- Os requisitos de governança são revistos e atualizados regularmente.

Antipadrões comuns:

- Sua organização exige que a conta raiz tenha autenticação multifator. Você não implementa esse requisito e a conta raiz é comprometida.

- Durante o design da workload, você escolhe um tipo de instância que não é aprovada pelo departamento de TI. Você não consegue iniciar a workload e precisa começar a reprojeta-la.
- É obrigatório que você tenha um plano de recuperação de desastres. Você não cria um, e a workload sofre uma interrupção prolongada.
- Sua equipe quer usar novas instâncias, mas seus requisitos de governança não foram atualizados para permiti-las.

Benefícios do estabelecimento desta prática recomendada:

- A aderência aos requisitos de governança alinha sua workload às políticas da organização como um todo.
- Os requisitos de governança refletem os padrões e as práticas recomendadas do setor para sua organização.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

Identifique o requisito de governança trabalhando com as partes interessadas e as organizações de governança. Inclua os requisitos de governança em sua workload. Prepare-se para demonstrar prova de que você seguiu os requisitos de governança.

Exemplo de clientes

Na Loja UmaEmpresa, a equipe de operações em nuvem trabalha com as partes interessadas dentro da organização para desenvolver requisitos de governança. Por exemplo, eles proíbem acesso SSH a instâncias do Amazon EC2. Caso as equipes precisem de acesso ao sistema, elas devem usar o AWS Systems Manager Session Manager. A equipe de operações em nuvem atualiza regularmente os requisitos de governança à medida que novos serviços são disponibilizados.

Etapas da implementação

1. Identifique as partes interessadas referentes à sua workload, incluindo quaisquer equipes centralizadas.
2. Trabalhe com as partes interessadas para identificar requisitos de governança.
3. Assim que gerar uma lista, priorize os itens de melhoria e comece a implementá-los na workload.

- a. Use serviços como o [AWS Config](#) para criar governança como código e validar se esses requisitos de governança são seguidos.
 - b. Se usar o [AWS Organizations](#), poderá utilizar políticas de controle de serviços para implementar requisitos de governança.
4. Forneça uma documentação que valide a implementação.

Nível de esforço do plano de implementação: médio. A implementação de requisitos de governança pode exigir a reformulação de sua workload.

Recursos

Práticas recomendadas relacionadas:

- [OPS01-BP04 Avaliar os requisitos de conformidade](#): a conformidade é como a governança, mas provém de fora da organização.

Documentos relacionados:

- [Guia de gerenciamento e governança do ambiente de nuvem da AWS](#)
- [Práticas recomendadas para políticas de controle de serviço do AWS Organizations](#)
- [Governança na Nuvem AWS: o equilíbrio entre agilidade e segurança](#)
- [O que é governança, risco e conformidade \(GRC\)?](#)

Vídeos relacionados:

- [Gerenciamento e governança da AWS: configuração, conformidade e auditoria – AWS Online Tech Talks](#)
- [AWS re:Inforce 2019: Governança da era da nuvem \(DEM12-R1\)](#)
- [AWS re:Invent 2020: Como alcançar a conformidade usando o AWS Config](#)
- [AWS re:Invent 2020: Governança ágil na AWS GovCloud \(US\)](#)

Exemplos relacionados:

- [Amostras de pacote de conformidade do AWS Config](#)

Serviços relacionados:

- [AWS Config](#)
- [AWS Organizations: políticas de controle de serviços](#)

OPS01-BP04 Avaliar os requisitos de conformidade

Os requisitos de conformidade normativos, setoriais e internos são um importante motivador para definir as prioridades de sua organização. Seu framework de conformidade pode impedir você de usar tecnologias ou localizações geográficas específicas. Realize a devida diligência se não for identificado nenhum framework de conformidade externo. Gere auditorias ou relatórios que validem a conformidade.

Se você anunciar que seu produto atende a padrões de conformidade específicos, deverá ter um processo interno para garantir a conformidade contínua. Os exemplos de padrões de conformidade incluem o PCI DSS, o FedRAMP e a HIPAA. Os padrões de conformidade aplicáveis são determinados por vários fatores, por exemplo, quais tipos de dados a solução armazena ou transmite e a quais regiões a solução oferece suporte.

Resultado desejado:

- Os requisitos de conformidade normativos, setoriais e internos são incorporados na seleção arquitetural.
- Você pode validar a conformidade e gerar relatórios de auditoria.

Antipadrões comuns:

- Partes da workload enquadram-se no framework Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI-DSS), mas a workload armazena dados de cartões de crédito não criptografados.
- Seus desenvolvedores e arquitetos de software não estão a par do framework de conformidade que sua organização deve adotar.
- A auditoria anual de Controle de Sistemas e Organizações: Tipo II (SOC2) será feita em breve e você não consegue verificar se esses controles estão em vigor.

Benefícios do estabelecimento desta prática recomendada:

- Avaliar e compreender os requisitos de conformidade que se aplicam à sua workload informará como você prioriza seus esforços para entregar valor empresarial.
- Você escolhe as localizações e tecnologias corretas, que são congruentes com seu framework de conformidade.
- Quando a workload é projetada para ser auditável, você tem a possibilidade de provar que está seguindo seu framework de conformidade.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

Implementar essa prática recomendada significa incorporar os requisitos de conformidade no processo de design da arquitetura. Os membros de sua equipe estão a par do framework de conformidade necessário. Você valida a conformidade de acordo com o framework.

Exemplo de clientes

A Loja UmaEmpresa armazena informações de cartão de crédito dos clientes. Os desenvolvedores da equipe de armazenamento de cartões sabem que eles precisam acatar o framework PCI-DSS. Eles tomaram medidas para verificar que as informações de cartão de crédito são armazenadas e acessadas com segurança, de acordo com o framework PCI-DSS. Todo ano, eles trabalham com a equipe de segurança para validar a conformidade.

Etapas da implementação

1. Trabalhe com as equipes de segurança e governança para determinar quais frameworks de conformidade normativos, setoriais ou internos a workload deve seguir. Incorpore os frameworks de conformidade em sua workload.
 - a. Valide a conformidade contínua dos recursos da AWS com serviços como o [AWS Compute Optimizer](#) e o [AWS Security Hub](#).
2. Instrua os membros da equipe sobre os requisitos de conformidade para que possam operar e expandir a workload de acordo com eles. Os requisitos de conformidade devem ser incluídos nas escolhas de arquitetura e tecnologia.
3. Dependendo do framework de conformidade, pode ser necessário gerar um relatório de auditoria ou conformidade. Trabalhe com sua organização para automatizar esse processo o máximo possível.

- a. Use serviços como o [AWS Audit Manager](#) para validar a conformidade e gerar relatórios de auditoria.
- b. Você pode baixar documentos de segurança e conformidade da AWS com o [AWS Artifact](#).

Nível de esforço do plano de implementação: médio. A implementação de frameworks de conformidade pode ser um desafio. A geração de relatórios de auditoria e de documentos de conformidade aumenta ainda mais complexidade.

Recursos

Práticas recomendadas relacionadas:

- [SEC01-BP03 Identificar e validar objetivos de controle](#): os objetivos de controle de segurança são uma parte importante da conformidade geral.
- [SEC01-BP06 Automatizar testes e validar controles de segurança em pipelines](#): como parte de seus pipelines, valide os controles de segurança. Você também pode gerar documentação de conformidade para novas mudanças.
- [SEC07-BP02 Definir controles de proteção de dados](#): muitos frameworks de conformidade têm políticas baseadas em processamento e armazenamento de dados.
- [SEC10-BP03 Preparar recursos forenses](#): às vezes é possível usar recursos forenses em auditoria de conformidade.

Documentos relacionados:

- [Centro de Conformidade da AWS](#)
- [Recursos de conformidade da AWS](#)
- [Whitepaper AWS: risco e conformidade](#)
- [Modelo de Responsabilidade Compartilhada da AWS](#)
- [Serviços da AWS no escopo por programa de conformidade](#)

Vídeos relacionados:

- [AWS re:Invent 2020: Como alcançar a conformidade usando o AWS Compute Optimizer](#)
- [AWS re:Invent 2021: Conformidade, garantia e auditoria](#)
- [AWS Summit ATL 2022: Implementação de conformidade, garantia e auditoria na AWS \(COP202\)](#)

Exemplos relacionados:

- [PCI DSS e Práticas recomendadas de segurança básica da AWS na AWS](#)

Serviços relacionados:

- [AWS Artifact](#)
- [AWS Audit Manager](#)
- [AWS Compute Optimizer](#)
- [AWS Security Hub](#)

OPS01-BP05 Avaliar o cenário de ameaças

Avalie as ameaças à empresa (por exemplo, concorrência, risco e passivos empresariais, riscos operacionais e ameaças à segurança da informação) e mantenha as informações atuais em um registro de risco. Inclua o impacto dos riscos ao determinar onde concentrar os esforços.

O [Well-Architected Framework](#) enfatiza o aprendizado, a medição e a melhoria. Ele fornece uma abordagem consistente para avaliar arquiteturas e implementar projetos que aumentarão em escala verticalmente ao longo do tempo. A AWS fornece o [AWS Well-Architected Tool](#) para ajudar você a analisar sua abordagem antes do desenvolvimento, o estado das cargas de trabalho antes da produção e o estado das cargas de trabalho na produção. Você pode compará-los com as práticas recomendadas de arquitetura mais recentes da AWS, monitorar o status geral das workloads e obter insights sobre possíveis riscos.

Os clientes da AWS estão qualificados para uma revisão orientada pelo Well-Architected de suas workloads de essenciais para [medir a arquitetura deles](#) em relação às práticas recomendadas da AWS. Os clientes do Enterprise Support estão qualificados para uma [Revisão de operações](#), projetada para ajudá-los a identificar lacunas em sua abordagem de operação na nuvem.

O envolvimento entre equipes dessas avaliações ajuda a estabelecer um entendimento comum de suas cargas de trabalho e como as funções da equipe contribuem para o sucesso. As necessidades identificadas pela avaliação podem ajudar a moldar suas prioridades.

[AWS Trusted Advisor](#) é uma ferramenta que fornece acesso a um conjunto principal de verificações que recomendam otimizações que podem ajudar a moldar suas prioridades. [Os clientes Business e Enterprise Support](#) recebem acesso a verificações adicionais com foco em segurança, confiabilidade, performance e otimização de custos que podem ajudar a moldar suas prioridades.

Antipadrões comuns:

- Você está usando uma versão antiga de uma biblioteca de software no seu produto. Você não está ciente das atualizações de segurança na biblioteca para problemas que podem ter um impacto indesejado na carga de trabalho.
- Seu concorrente acabou de lançar uma versão do produto que lida com muitas das reclamações de seus clientes sobre seu produto. Você não priorizou a abordagem de nenhum desses problemas conhecidos.
- Os reguladores buscam empresas como a sua que não estejam em conformidade com os requisitos de conformidade normativa legais. Você não priorizou a abordagem de nenhum de seus requisitos de conformidade pendentes.

Benefícios do estabelecimento desta prática recomendada: Identificar e compreender as ameaças à sua organização e carga de trabalho permite determinar quais ameaças devem ser resolvidas, a prioridade delas e os recursos necessários para isso.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

- Avaliar o cenário de ameaças aos negócios: avalie as ameaças aos negócios (como concorrência, riscos e responsabilidades comerciais, riscos operacionais e ameaças à segurança das informações), para que você possa incluir o impacto dessas ameaças ao determinar onde concentrar esforços.
 - [Boletins de segurança mais recentes da AWS](#)
 - [AWS Trusted Advisor](#)
- Manter um modelo de ameaças: estabeleça e mantenha um modelo de ameaças que identifique possíveis ameaças, mitigações planejadas e implementadas e a prioridade delas. Analise a probabilidade de as ameaças se manifestarem como incidentes, o custo de recuperação desses incidentes, o dano esperado causado e o custo para evitar esses incidentes. Revise as prioridades à medida que o conteúdo do modelo de ameaça muda.

Recursos

Documentos relacionados:

- [Conformidade da Nuvem AWS](#)

- [Boletins de segurança mais recentes da AWS](#)
- [AWS Trusted Advisor](#)

OPS01-BP06 Avalie as compensações

Avalie o impacto das compensações entre interesses concorrentes ou abordagens alternativas para ajudar a tomar decisões embasadas ao determinar onde concentrar os esforços ou escolher um plano de ação. Por exemplo, a aceleração da velocidade de entrada no mercado de novos recursos pode ser enfatizada em relação à otimização de custos, ou você pode escolher um banco de dados relacional para dados não relacionais para simplificar o esforço de migração de um sistema, em vez de migrar para um banco de dados otimizado para seu tipo de dados e atualizar seu aplicativo.

A AWS pode ajudar a educar suas equipes sobre a AWS e seus serviços para aumentar a compreensão de como suas escolhas podem ter um impacto na workload. Você deve usar os recursos fornecidos pelo [AWS Support](#) ([Centro de Conhecimentos da AWS](#), [Fóruns de discussão da AWS](#) e [AWS Support Center](#)) e pela [documentação da AWS](#) para instruir suas equipes. Entre em contato com o AWS Support por meio do AWS Support Center para obter ajuda com relação às suas dúvidas sobre a AWS.

A AWS também compartilha as práticas recomendadas e os padrões que aprendemos durante a operação da AWS na [Amazon Builders' Library](#). Uma variedade de outras informações úteis está disponível no [Blog da AWS](#) e [O podcast oficial da AWS](#).

Antipadrões comuns:

- Você está usando um banco de dados relacional para gerenciar séries temporais e dados não relacionais. Existem opções de banco de dados otimizadas para oferecer suporte aos tipos de dados que você está usando, mas você não tem conhecimento dos benefícios, pois não avaliou as compensações entre soluções.
- Seus investidores solicitam que você demonstre conformidade com os Padrões de segurança de dados do setor de cartões de pagamento (PCI DSS). Você não considera as compensações entre atender à solicitação deles e continuar com seus esforços de desenvolvimento atuais. Em vez disso, prossiga com seus esforços de desenvolvimento sem demonstrar conformidade. Seus investidores interrompem o suporte da sua empresa devido a preocupações com a segurança da sua plataforma e com os investimentos deles.

Benefícios do estabelecimento desta prática recomendada: Entender as implicações e as consequências de suas escolhas permite que você priorize suas opções.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Médio

Orientações para a implementação

- **Avaliar as compensações:** avalie o impacto das compensações entre as partes interessadas concorrentes para ajudar a tomar decisões embasadas ao determinar onde concentrar esforços. Por exemplo, a aceleração da velocidade de introdução no mercado de novos recursos pode ser enfatizada sobre a otimização de custos.
- A AWS pode ajudar a educar suas equipes sobre a AWS e seus serviços para aumentar a compreensão de como suas escolhas podem ter um impacto na workload. Use os recursos fornecidos pelo AWS Support (Centro de Conhecimentos da AWS, Fóruns de discussão da AWS e AWS Support Center) e pela documentação da AWS para instruir suas equipes. Entre em contato com o AWS Support por meio do AWS Support Center para obter ajuda com relação às suas dúvidas sobre a AWS.
- A AWS também compartilha as práticas recomendadas e os padrões que aprendemos durante a operação da AWS na Amazon Builders' Library. Uma grande variedade de outras informações úteis está disponível no Blog da AWS e no podcast oficial da AWS.

Recursos

Documentos relacionados:

- [Blog da AWS](#)
- [Conformidade da Nuvem AWS](#)
- [Fóruns de discussão da AWS](#)
- [documentação da AWS](#)
- [Centro de Conhecimentos da AWS](#)
- [AWS Support](#)
- [AWS Support Center](#)
- [Amazon Builders' Library](#)
- [O podcast oficial da AWS](#)

OPS01-BP07 Gerenciar os benefícios e os riscos

Gerencie benefícios e riscos para tomar decisões informadas ao determinar onde concentrar os esforços. Pode ser benéfico, por exemplo, implantar uma carga de trabalho com problemas não resolvidos a fim de disponibilizar recursos novos e significativos aos clientes. Talvez seja possível mitigar os riscos associados ou talvez seja inaceitável permitir que um risco permaneça; nesse caso, você tomará as devidas medidas para resolver o risco.

Em determinado momento, talvez você deseje destacar um pequeno subconjunto de prioridades. Use uma abordagem equilibrada em longo prazo para garantir o desenvolvimento dos recursos necessários e o gerenciamento de riscos. Atualize suas prioridades conforme as necessidades mudam

Antipadrões comuns:

- Um de seus desenvolvedores encontrou na Internet, uma biblioteca que faz tudo o que você precisa, e você decidiu incluí-la. Você não avaliou os riscos de adoção dessa biblioteca de uma origem desconhecida e não sabe se ela contém vulnerabilidades ou código mal-intencionado.
- Você decidiu desenvolver e implantar um novo recurso em vez de corrigir um problema existente. Você não avaliou os riscos de continuar com o problema até que o recurso seja implantado e não sabe qual será o impacto nos seus clientes.
- Você decidiu não implantar um recurso solicitado frequentemente pelos clientes devido a preocupações não especificadas da sua equipe de conformidade.

Benefícios do estabelecimento desta prática recomendada: Identificar os benefícios disponíveis das suas escolhas e estar ciente dos riscos para a sua organização permite que você tome decisões bem embasadas.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Baixo

Orientações para a implementação

- Gerenciar os benefícios e os riscos: equilibre os benefícios das decisões em relação aos riscos envolvidos.
 - Identificar os benefícios: identifique os benefícios com base nas metas, necessidades e prioridades da empresa. Os exemplos incluem tempo de colocação no mercado, segurança, confiabilidade, performance e custo.

- Identificar os riscos: identifique os riscos com base nas metas, necessidades e prioridades da empresa. Os exemplos incluem tempo de colocação no mercado, segurança, confiabilidade, performance e custo.
- Avaliar os benefícios em relação aos riscos e tomar decisões embasadas: determine o impacto dos benefícios e dos riscos com base nas metas, necessidades e prioridades das principais partes interessadas, incluindo os negócios, o desenvolvimento e as operações. Avalie o valor do benefício em relação à probabilidade de realização do risco e o custo do seu impacto. Por exemplo, enfatizar a velocidade de entrada no mercado em vez da confiabilidade pode oferecer vantagem competitiva. No entanto, isso pode resultar em tempo de atividade reduzido se houver problemas de confiabilidade.

Modelo operacional

Suas equipes devem compreender o papel delas na obtenção de resultados empresariais. As equipes precisam entender o papel delas no êxito de outras equipes e a função das outras equipes no êxito delas e ter objetivos compartilhados. Entender a responsabilidade, a propriedade, como as decisões são tomadas e quem tem autoridade para tomar decisões ajudará a concentrar os esforços e maximizar os benefícios das suas equipes.

As necessidades de uma equipe são modeladas pelo setor, pela organização, pela formação da equipe e pelas características da carga de trabalho. Não é sensato esperar que um modelo operacional único seja capaz de dar suporte a todas as equipes e suas respectivas cargas de trabalho.

O número de modelos operacionais presentes em uma organização provavelmente aumentará com o número de equipes de desenvolvimento. Pode ser necessário usar uma combinação de modelos operacionais.

A adoção de padrões e o consumo de serviços podem simplificar as operações e limitar a carga de suporte em seu modelo operacional. O benefício dos esforços de desenvolvimento em padrões compartilhados é ampliado pelo número de equipes que adotaram o padrão e que adotarão novos recursos.

É essencial que existam mecanismos para solicitar adições, alterações e exceções aos padrões de suporte às atividades das equipes. Sem essa opção, os padrões se tornam uma restrição à inovação. As solicitações devem ser aprovadas quando viáveis e determinadas como apropriadas após uma avaliação dos benefícios e riscos.

Um conjunto bem definido de responsabilidades reduz a frequência de esforços conflitantes e redundantes. Os resultados empresariais são mais fáceis de alcançar quando há um bom alinhamento e bons relacionamentos entre as equipes de negócios, desenvolvimento e operações.

Representações do modelo operacional 2 por 2

Essas representações do modelo operacional 2 por 2 são ilustrações para ajudar a compreender as relações entre as equipes em seu ambiente. Esses diagramas se concentram em quem faz o quê e nos relacionamentos entre as equipes, mas também discutiremos a governança e tomada de decisões no contexto desses exemplos.

Nossas equipes podem ter responsabilidades em várias partes de diversos modelos, dependendo das workloads às quais oferecem suporte. Talvez você queira separar áreas de disciplina mais especializadas do que as de alto nível descritas. Existem possibilidades infinitas de variação nesses modelos com base na forma como você separa ou agrega atividades ou sobrepõe equipes e fornece detalhes mais específicos.

Talvez você identifique que tem recursos sobrepostos ou não reconhecidos em equipes que podem fornecer vantagem adicional ou resultar em eficiências. Você também pode identificar necessidades não atendidas na sua organização e que você planeja atender no futuro.

Ao avaliar a mudança organizacional, examine as diferenças entre modelos, onde suas equipes individuais residem nos modelos (agora e depois da mudança), como o relacionamento e as responsabilidades das equipes mudarão e se os benefícios compensam o impacto na sua organização.

Você pode ter êxito ao usar cada um dos quatro modelos operacionais a seguir. Alguns modelos são mais apropriados para casos de uso específicos ou em pontos específicos do seu desenvolvimento. Alguns desses modelos podem fornecer vantagens em relação aos modelos atualmente usados no seu ambiente.

Tópicos

- [Modelo operacional totalmente separado](#)
- [Engenharia e operações de aplicações separadas \(AEO\) e engenharia e operações de infraestrutura \(IEO\) com governança centralizada](#)
- [AEO e IEO separadas com governança centralizada e um provedor de serviços](#)
- [AEO e IEO separadas com governança centralizada e um provedor de serviços e parceiro de consultoria interno](#)

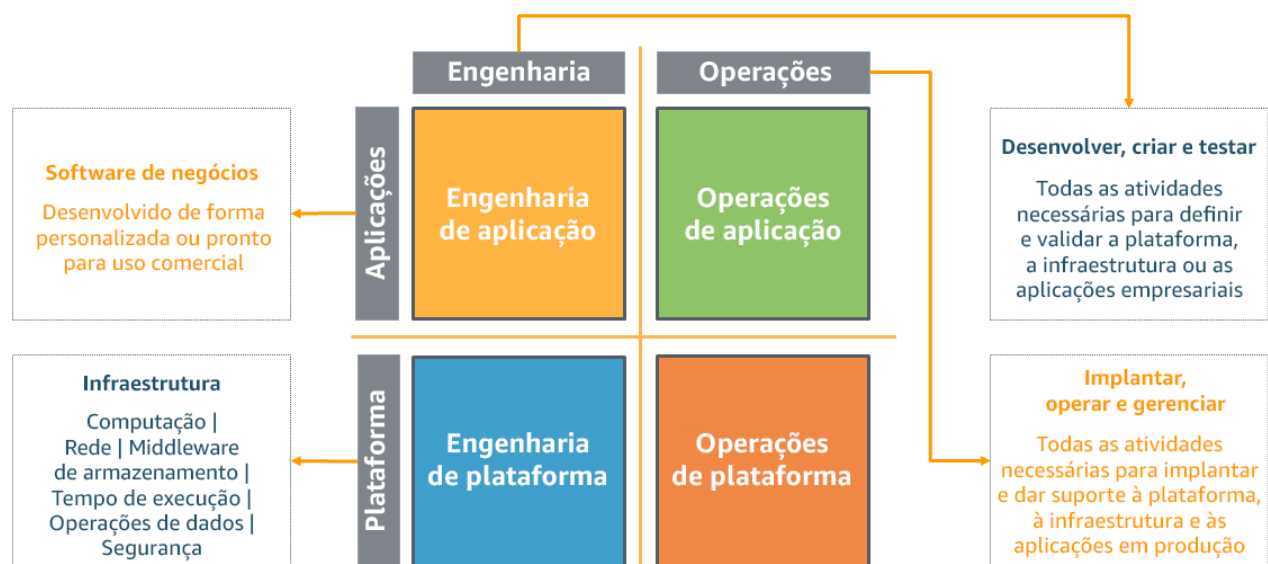
- [AEO e IEO separadas com governança descentralizada](#)

Modelo operacional totalmente separado

No diagrama a seguir, no eixo vertical, há "Aplicativos" e "Infraestrutura". "Aplicativos" referem-se à carga de trabalho que atende a um resultado comercial e podem ser softwares personalizados desenvolvidos ou adquiridos. "Infraestrutura" refere-se à infraestrutura física e virtual e a outros softwares compatíveis com essa carga de trabalho.

No eixo horizontal, temos "Engenharia" e "Operações". "Engenharia" refere-se ao desenvolvimento, à criação e ao teste de aplicativos e infraestrutura. "Operações" abrange a implantação, a atualização e o suporte contínuo de aplicativos e da infraestrutura.

Modelo tradicional



Muitas organizações adotam esse modelo "totalmente separado". As atividades em cada quadrante são realizadas por uma equipe separada. O trabalho é transmitido entre equipes por meio de mecanismos como solicitações de trabalho, filas de trabalho, tíquetes ou um sistema de gerenciamento de serviços de TI (ITSM).

A transição de tarefas para ou entre equipes aumenta a complexidade e cria gargalos e atrasos. As solicitações podem ser atrasadas até que sejam uma prioridade. Os defeitos identificados com atraso

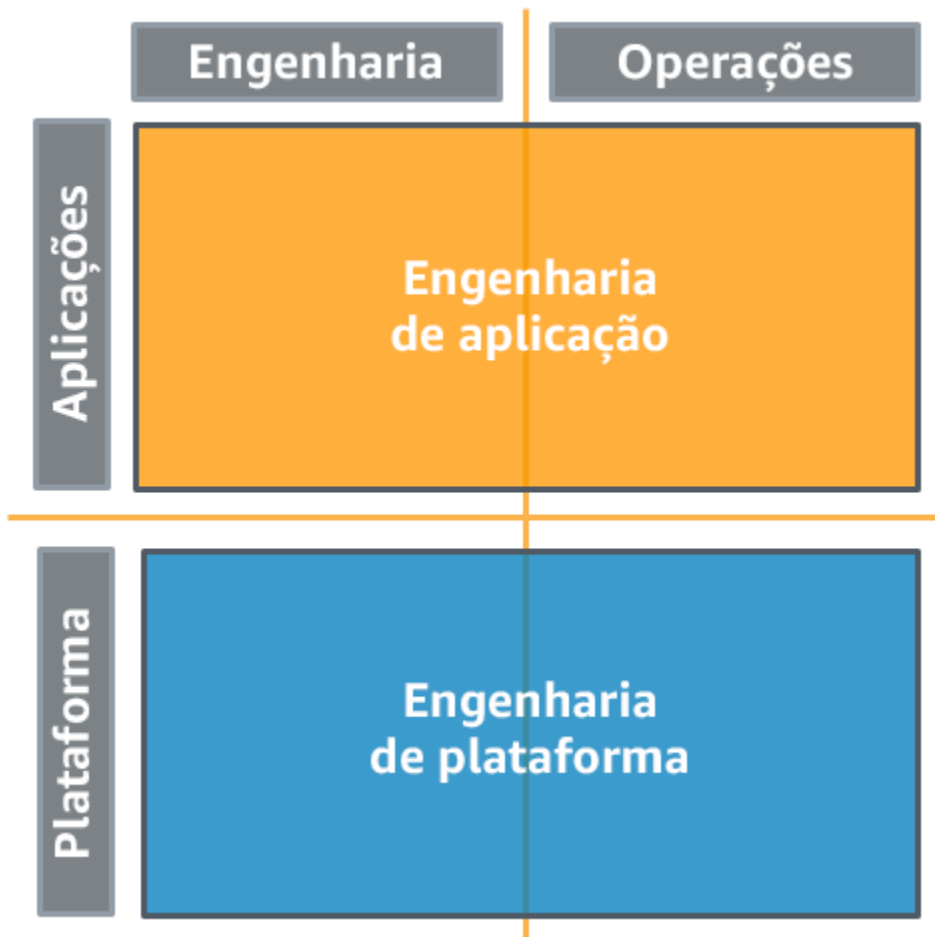
podem exigir retrabalho significativo e talvez precisem passar novamente pelas mesmas equipes e suas funções. Se houver incidentes que exijam ação das equipes de engenharia, as respostas delas serão atrasadas pela atividade de entrega.

Há um risco maior de desalinhamento quando as equipes de negócios, desenvolvimento e operações são organizadas em torno das atividades ou funções executadas. Isso pode fazer com que as equipes se concentrem em responsabilidades específicas, em vez de buscarem alcançar resultados empresariais. As equipes podem ter especialização limitada e podem estar isoladas em nível físico ou lógico, o que dificulta a comunicação e a colaboração.

Engenharia e operações de aplicações separadas (AEO) e engenharia e operações de infraestrutura (IEO) com governança centralizada

Esse modelo de "AEO e IEO separados" segue uma metodologia "você cria, você executa".

Seus engenheiros e desenvolvedores de aplicativos executam a engenharia e a operação de cargas de trabalho. Da mesma forma, seus engenheiros de infraestrutura executam a engenharia e a operação das plataformas usadas para dar suporte às equipes de aplicativos.



Neste exemplo, vamos tratar a governança como centralizada. Os padrões são distribuídos, fornecidos ou compartilhados com as equipes de aplicativos.

Você deve usar ferramentas ou serviços que permitam controlar centralmente seus ambientes em todas as contas, como o [AWS Organizations](#). Serviços como o [AWS Control Tower](#) expandem esse recurso de gerenciamento, permitindo que você defina esquemas (compatíveis com modelos operacionais) para a configuração de contas, aplique governança contínua usando o AWS Organizations e automatize o provisionamento de novas contas.

A metologia "você cria, você executa" não significa que a equipe do aplicativo é responsável pela pilha completa, pela cadeia de ferramentas e pela plataforma.

A equipe de engenharia de plataforma fornece um conjunto padronizado de serviços (por exemplo, ferramentas de desenvolvimento, ferramentas de monitoramento, ferramentas de backup e recuperação e rede) para a equipe de aplicativos. A equipe de plataforma também pode fornecer à

equipe de aplicativos acesso a serviços de provedor de nuvem aprovados, configurações específicas ou ambos.

Mecanismos que fornecem um recurso de autoatendimento para implantação de serviços e configurações aprovados, como o [Service Catalog](#), podem ajudar a limitar os atrasos associados ao atendimento de solicitações ao mesmo tempo em que impõem a governança.

A equipe de plataforma proporciona visibilidade completa da pilha para que as equipes de aplicativos possam diferenciar problemas em seus componentes de aplicativos e os serviços e componentes de infraestrutura que seus aplicativos consomem. A equipe de plataforma também pode fornecer assistência para configurar esses serviços e orientações sobre como melhorar as operações das equipes de aplicativos.

Como discutido anteriormente, é essencial que existam mecanismos para que a equipe de aplicativos solicite adições, alterações e exceções aos padrões de suporte às atividades das equipes e à inovação dos aplicativos delas.

O modelo de AEO e IEO separados proporciona bons ciclos de comentários para as equipes de aplicativos. As operações diárias de uma carga de trabalho aumentam o contato com os clientes por interação direta ou indireta por meio de solicitações de suporte e recursos. Essa visibilidade aumentada permite que as equipes de aplicativos solucionem problemas mais rapidamente. O envolvimento mais profundo e o relacionamento mais próximo fornecem informações sobre as necessidades dos clientes e permitem uma inovação mais rápida.

Tudo isso também é válido para a equipe de plataforma que dá suporte às equipes de aplicativos.

Os padrões adotados podem ser pré-aprovados para uso, reduzindo a quantidade de análise necessária para entrar em produção. O consumo de padrões compatíveis e testados fornecidos pela equipe da plataforma pode reduzir a frequência de problemas com esses serviços. A adoção de padrões permite que as equipes de aplicativos se concentrem em diferenciar suas cargas de trabalho.

AEO e IEO separadas com governança centralizada e um provedor de serviços

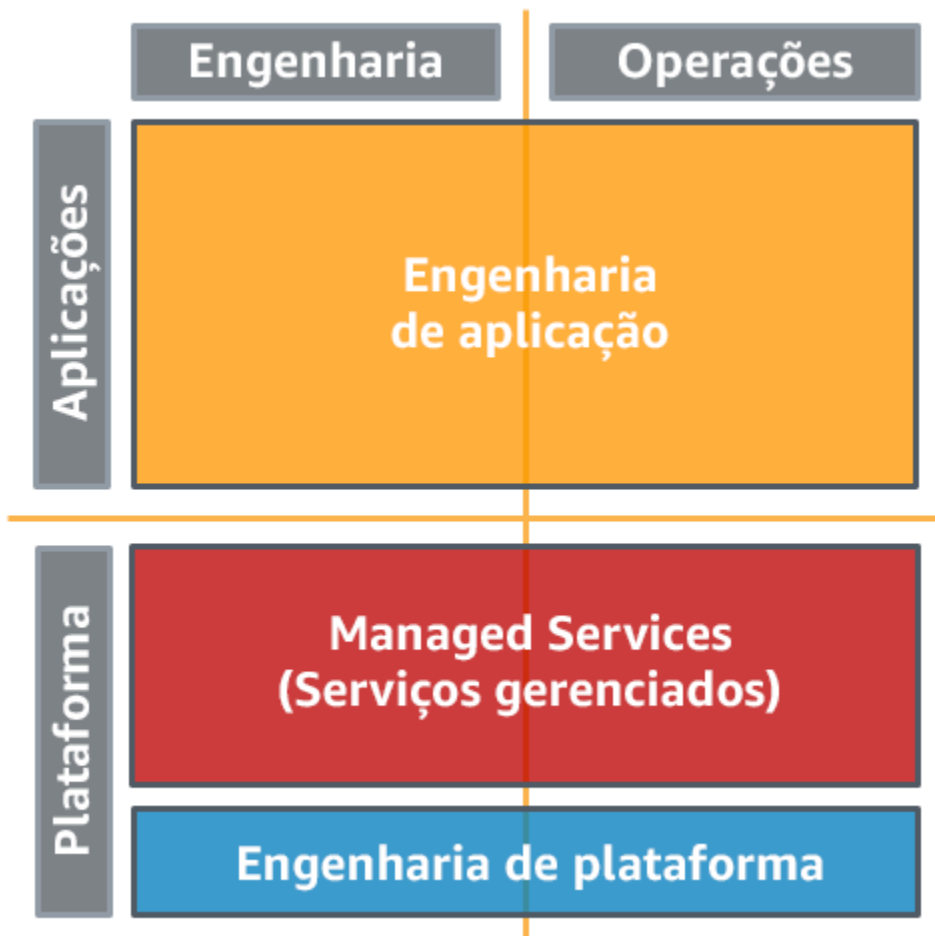
Esse modelo de "AEO e IEO separados" segue uma metodologia "você cria, você executa".

Seus engenheiros e desenvolvedores de aplicativos executam a engenharia e a operação de cargas de trabalho.

Sua organização pode não ter as habilidades ou os membros da equipe necessários para dar suporte a uma equipe dedicada de engenharia e operações de plataforma, ou talvez você não deseje investir tempo e esforço para isso.

Como alternativa, você pode ter uma equipe de plataforma focada na criação de recursos que diferenciam a sua empresa, mas deseja transferir para terceiros as operações diárias que não geram diferenciação.

Provedores de serviços gerenciados, como o [AWS Managed Services](#), [Parceiros do AWS Managed Services](#) ou Provedores de serviços gerenciados na [Rede de Parceiros da AWS](#), fornecem especialização na implementação de ambientes de nuvem e dão suporte aos seus requisitos de segurança e conformidade e objetivos de negócios.



Para essa variação, vamos tratar a governança como centralizada e gerenciada pela equipe de plataforma, com a criação de contas e políticas gerenciadas com o AWS Organizations e o AWS Control Tower.

Esse modelo exige que você modifique seus mecanismos para trabalhar com os mecanismos do seu provedor de serviços. Ele não aborda os gargalos e atrasos criados pela transição de tarefas entre equipes, incluindo seu provedor de serviços, ou o possível retrabalho relacionado à identificação tardia de defeitos.

Você obtém a vantagem dos padrões, das melhores práticas, dos processos e da experiência dos seus provedores. Também obtém os benefícios do desenvolvimento contínuo das ofertas de serviços deles.

A adição de serviços gerenciados ao seu modelo operacional pode economizar tempo e recursos, além de permitir que você mantenha as equipes internas reduzidas e focadas em resultados estratégicos que diferenciarão seus negócios, em vez de desenvolver novas habilidades e recursos.

AEO e IEO separadas com governança centralizada e um provedor de serviços e parceiro de consultoria interno

Esse modelo de “AEO e IEO separadas” segue a metodologia “você cria, você executa”.

Você quer que as suas equipes de aplicações executem as atividades de engenharia e de operações para suas workloads e adotem uma cultura mais DevOps.

As equipes de aplicações podem estar em processo de migração, de adoção da nuvem ou de modernização das suas workloads, e não ter as habilidades necessárias para oferecer suporte adequado à nuvem e às operações em nuvem. Essa falta de habilidades ou de familiaridade da equipe de aplicações pode ser uma barreira para seus esforços.

Para resolver esse problema, estabeleça uma equipe de Centro de Capacitação em Nuvem (CCoE) que forneça um fórum para fazer perguntas, discutir necessidades e identificar soluções. Dependendo das necessidades da sua organização, o CCoE também pode ser uma equipe de especialistas ou uma equipe virtual com participantes selecionados de toda a empresa. O CCoE habilita as equipes para a transformação para a nuvem, estabelece governança centralizada da nuvem e define os padrões de gerenciamento de contas e da organização. As equipes também identificam arquiteturas de referência bem-sucedidas e padrões para uso da empresa.

Nós nos referimos ao CCoE como Centro de Capacitação em Nuvem, em vez do Centro de Excelência em Nuvem, mais comum, a fim de enfatizar a capacitação para o sucesso das equipes que recebem apoio e a concretização de resultados empresariais.

A equipe de engenharia cria os recursos principais da plataforma com base nos padrões para a adoção das equipes de aplicações. A equipe codifica as arquiteturas e os padrões de referência

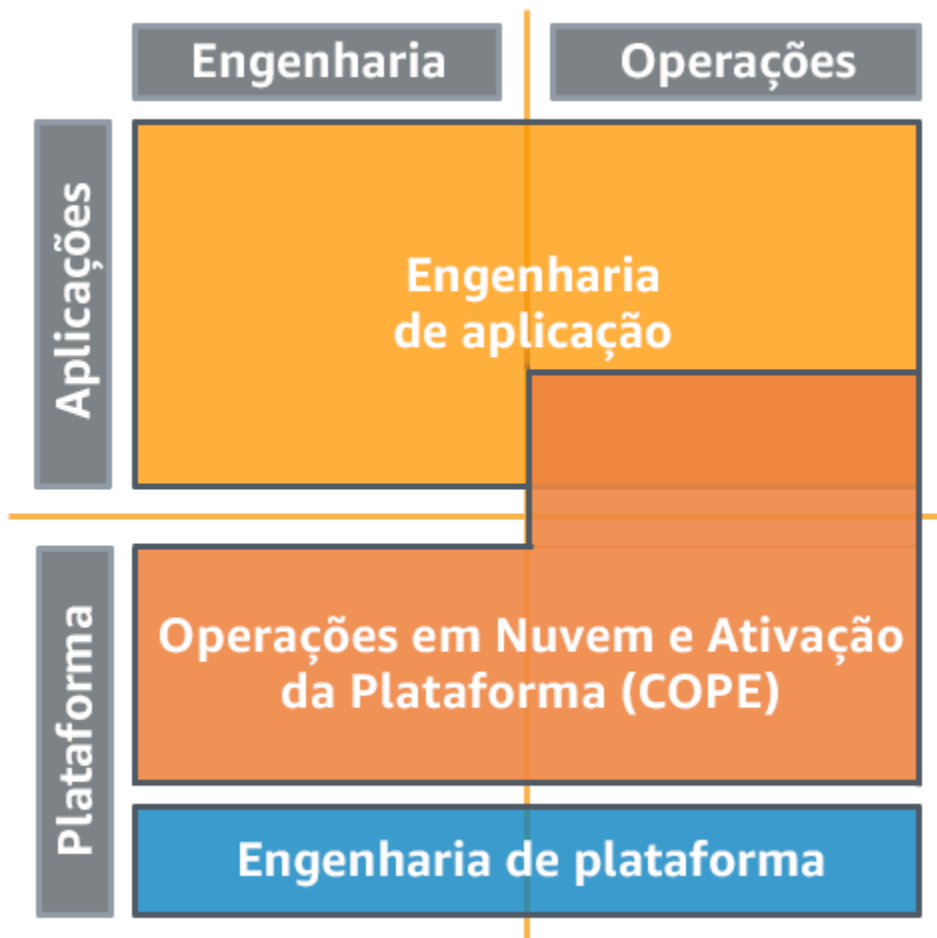
da empresa fornecidos às equipes de aplicações por meio de um mecanismo de autoatendimento. Usando um serviço como o AWS Service Catalog, as equipes de aplicações podem implantar arquiteturas, padrões, serviços e configurações de referência aprovadas, compatíveis com a governança centralizada e os padrões de segurança.

Além disso, a equipe de engenharia da plataforma fornece um conjunto padronizado de serviços (por exemplo, ferramentas de desenvolvimento, ferramentas de monitoramento, ferramentas de backup e recuperação e rede) às equipes de aplicações.

Sua organização tem um “MSP e parceiro de consultoria interno” que gerencia e oferece suporte aos serviços padronizados, e fornece assistência às equipes de aplicações que estabelecem sua presença na nuvem com base nas arquiteturas e padrões de referência. Essa equipe de “Operações em Nuvem e Ativação da Plataforma (COPE)” trabalha com as equipes de aplicações para ajudá-las a estabelecer as operações de linha de base. Por sua vez, as equipes de aplicações assumem maior responsabilidade progressivamente em relação aos respectivos sistemas e recursos. A equipe de COPE motiva a melhoria contínua com as equipes do CCoE e de engenharia de plataforma, e atuam como defensores das equipes de aplicações.

As equipes de aplicações obtêm assistência para configurar os ambientes, os pipelines de CI/CD, o gerenciamento de mudanças, a observabilidade e o monitoramento e, com a equipe de COPE, estabelecem os processos de gerenciamento de incidentes e eventos integrados com os da empresa, conforme necessário. A equipe de COPE colabora com as equipes de aplicações na performance dessas atividades de operações, e encerra gradualmente o envolvimento à medida que as equipes de aplicações assumem as responsabilidades.

A equipe de aplicações se beneficia das habilidades da equipe de COPE e das lições aprendidas pela organização. Elas são protegidas pelas barreiras de proteção estabelecidas pela governança centralizada. As equipes de aplicações se baseiam em sucessos reconhecidos e obtêm o benefício do desenvolvimento contínuo dos padrões da organização que adotaram. Elas obtêm um insight melhor da operação da workload por meio do estabelecimento da observabilidade e do monitoramento, e são mais capazes de compreender o impacto das alterações que elas fazem nas workloads.



A equipe de COPE retém o acesso necessário para oferecer suporte às atividades de operações, fornece uma visão das operações empresariais que abrange as equipes de aplicações e suporte ao gerenciamento de incidentes críticos. A equipe de COPE retém a responsabilidade por atividades consideradas de forma indistinta como pesadas, que atendem por meio de soluções padrão compatíveis em escala. Ela também continua a gerenciar as operações consideradas como automatizadas e programáticas para as equipes de aplicações, para que elas possam focalizar na distinção de suas aplicações.

Você obtém a vantagem dos padrões, práticas recomendadas, processo e especialização de sua organização derivados do sucesso de suas equipes. Você estabelece um mecanismo para replicar esses padrões bem-sucedidos para adoção por novas equipes ou para a modernização na nuvem. Esse modelo enfatiza a habilidade da equipe de COPE de ajudar a equipe de aplicações a obter artefatos e conhecimento de transições estabelecidos. Ele reduz as cargas operacionais das equipes de aplicações com o risco de essas equipes não se tornarem em grande parte independentes.

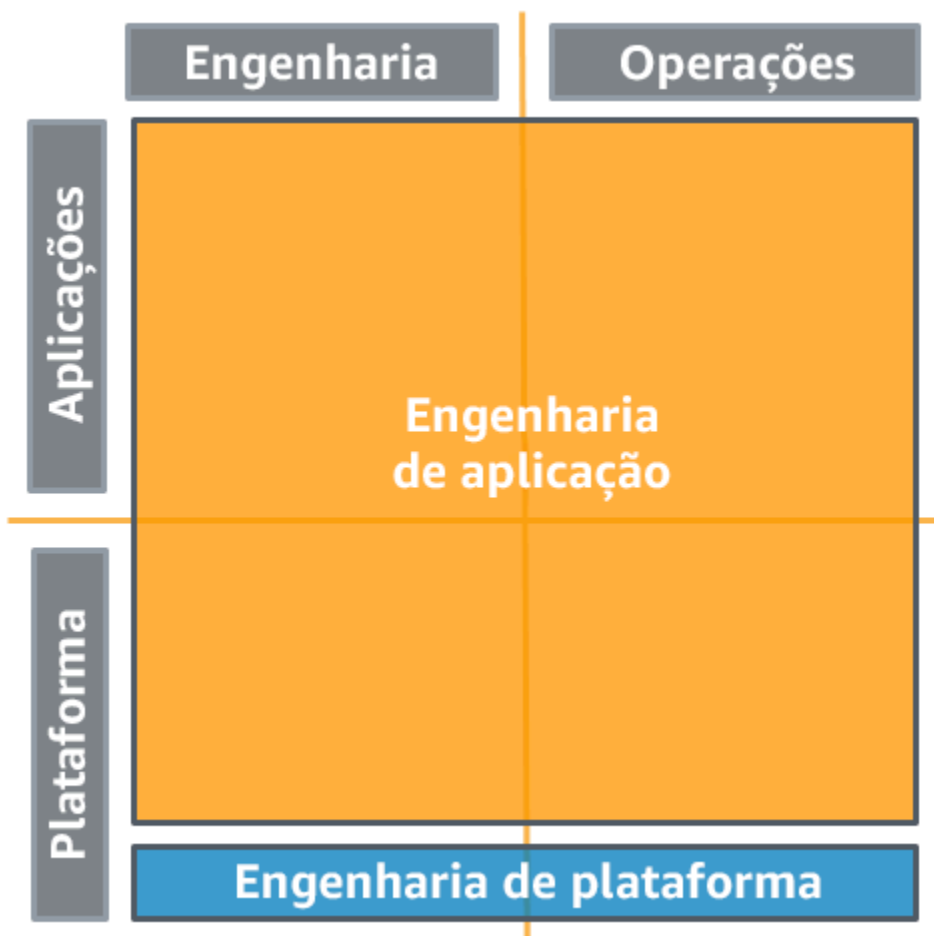
Estabelece relacionamentos entre as equipes de CCoE, de COPE e de aplicações, criando um loop de feedbacks para atender às evoluções e inovações futuras.

O estabelecimento de equipes de CCoE e de COPE, bem como a definição dos padrões de toda a organização, pode facilitar a adoção da nuvem e apoiar as iniciativas de modernização. Ao fornecer o suporte adicional de uma equipe de COPE, que atua como consultora e parceira para suas equipes de aplicações, você pode remover barreiras que atrasam a adoção dos promissores recursos da nuvem.

AEO e IEO separadas com governança descentralizada

Esse modelo de "AEO e IEO separados" segue uma metodologia "você cria, você executa".

Seus engenheiros e desenvolvedores de aplicativos executam a engenharia e a operação de cargas de trabalho. Da mesma forma, seus engenheiros de infraestrutura executam a engenharia e a operação das plataformas usadas para dar suporte às equipes de aplicativos.



Neste exemplo, vamos tratar a governança como descentralizada.

Os padrões ainda são distribuídos, fornecidos ou compartilhados com equipes de aplicativos pela equipe de plataforma, mas as equipes de aplicativos podem projetar e operar novos recursos de plataforma para apoiar a carga de trabalho.

Nesse modelo, há menos restrições para a equipe de aplicativos, mas isso vem com um aumento significativo nas responsabilidades. É preciso ter habilidades adicionais (e possivelmente mais membros da equipe) para dar suporte aos recursos adicionais da plataforma. O risco de retrabalho significativo aumentará se os conjuntos de habilidades não forem adequados e se os defeitos não forem reconhecidos com antecedência.

Você deve aplicar políticas que não sejam especificamente delegadas às equipes de aplicativos. Use ferramentas ou serviços que permitam controlar centralmente seus ambientes em várias contas, como o [AWS Organizations](#). Serviços como o [AWS Control Tower](#) expandem esse recurso de gerenciamento, permitindo definir esquemas (compatíveis com modelos operacionais) para a configuração de contas, a aplicação de governança contínua usando o AWS Organizations e a automatização do provisionamento de novas contas.

É benéfico ter mecanismos para que a equipe de aplicativos solicite adições e alterações em padrões. Eles podem colaborar com novos padrões que ofereçam benefícios a outras equipes de aplicativos. As equipes de plataforma podem decidir que fornecer suporte direto para esses recursos adicionais é um suporte eficaz para resultados empresariais.

Esse modelo reduz as restrições de inovação com requisitos significativos de habilidades e membros da equipe. Ele aborda muitos dos gargalos e atrasos criados pela transição de tarefas entre equipes e, ao mesmo tempo, promove o desenvolvimento de relacionamentos eficazes entre equipes e clientes.

Relacionamentos e propriedade

Seu modelo operacional define os relacionamentos entre equipes e dá suporte à propriedade e à responsabilidade identificáveis.

Práticas recomendadas

- [OPS02-BP01 Recursos com proprietários identificados](#)
- [OPS02-BP02 Processos e procedimentos com proprietários identificados](#)
- [OPS02-BP03 Atividades de operações com proprietários identificados responsáveis pela performance](#)

- [OPS02-BP04 Os membros da equipe sabem pelo que são responsáveis](#)
- [OPS02-BP05 Existem mecanismos para identificar a responsabilidade e a propriedade](#)
- [OPS02-BP06 Mecanismos existem para solicitar adições, alterações e exceções](#)
- [OPS02-BP07 As responsabilidades entre as equipes são predefinidas ou negociadas](#)

OPS02-BP01 Recursos com proprietários identificados

Os recursos para sua workload devem ter proprietários identificados para controle de alterações, resolução de problemas e outras funções. Atribuem-se proprietários para workloads, contas, infraestrutura, plataformas e aplicações. A propriedade é registrada usando ferramentas como um registro central ou metadados anexados aos recursos. O valor empresarial dos componentes indica os processos e procedimentos aplicados a eles.

Resultado desejado:

- Os recursos têm proprietários identificados usando metadados ou um registro central.
- Os membros da equipe podem identificar quem é proprietários dos recursos.
- As contas têm um único proprietário quando possível.

Antipadrões comuns:

- Os contatos alternativos para suas Contas da AWS não estão preenchidos.
- Os recursos não têm as tags que identificam as equipes às quais eles pertencem.
- Você tem uma fila ITSM sem mapeamento de e-mail.
- Duas equipes são proprietárias de uma mesma parte essencial da infraestrutura.

Benefícios do estabelecimento desta prática recomendada:

- O controle de alterações para recursos é fácil com a atribuição de propriedade.
- Você pode envolver os proprietários corretos na resolução de problemas.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

Defina o que significa propriedade para os casos de uso de recursos em seu ambiente. A propriedade pode se referir a quem supervisiona alterações no recurso e apoia o recurso durante a resolução de problemas ou a quem é responsável pela parte financeira. Especifique e registre proprietários para recursos, incluindo nome, informações de contato, organização e equipe.

Exemplo de clientes

A Loja UmaEmpresa define propriedade como a equipe ou a pessoa proprietária das alterações e do suporte para os recursos. Eles utilizam o AWS Organizations para gerenciar as Contas da AWS. Os contatos de conta alternativos são configurados usando as caixas de entrada de grupo. Cada fila ITSM é mapeada para um alias de e-mail. As tags identificam quem é proprietário dos recursos da AWS. Para outras plataformas e infraestrutura, eles têm uma página de wiki que identifica informações sobre propriedade e contato.

Etapas da implementação

1. Para começar, identifique a propriedade sobre sua organização. A propriedade pode estar relacionada a quem é proprietário do risco referente ao recurso, a quem é proprietário das alterações referentes ao recurso ou a quem apoia o recurso na resolução de problemas. Propriedade também pode significar propriedade financeira ou administrativa pelo recurso.
2. Use o [AWS Organizations](#) para gerenciar contas. Você pode gerenciar contatos alternativos centralmente para as suas contas.
 - a. O uso de endereços de e-mail ou de números de telefones de propriedade da empresa para informações de contato permite acessá-los mesmo quando os indivíduos aos quais eles pertencem não estiverem mais na organização. Por exemplo, crie listas de distribuição de e-mail separadas para faturamento, operações e segurança, e configure-as como contatos de Faturamento, Segurança e Operações em cada Conta da AWS ativa. Várias pessoas receberão notificações da AWS e poderão respondê-las, mesmo que alguém esteja de férias, mude de função ou saia da empresa.
 - b. Se uma conta não for gerenciada pelo [AWS Organizations](#), os contatos alternativos para contas ajudarão a AWS a entrar em contato com o pessoal apropriado, se necessário. Configure os contatos alternativos da conta para apontar para um grupo em vez de uma pessoa.
3. Use tags para identificar proprietários de recursos da AWS. Você pode especificar os proprietários e as respectivas informações de contato em tags separadas.
 - a. Pode usar regras do [AWS Config](#) para reforçar que os recursos têm as tags de propriedade necessárias.

- b. Para obter orientações detalhadas sobre como elaborar uma estratégia de marcação para sua organização, consulte o [whitepaper Práticas recomendadas de marcação da AWS](#).
4. Para outros recursos, plataformas e infraestrutura, crie uma documentação que identifique a propriedade. Ela deve ser acessível a todos os membros da equipe.

Nível de esforço do plano de implementação: baixo. Utilize informações de contato da conta e tags para atribuir propriedade a recursos da AWS. Para outros recursos, você pode usar algo simples como uma tabela em uma wiki para registrar a propriedade e informações de contato ou usar uma ferramenta de ITSM para mapear a propriedade.

Recursos

Práticas recomendadas relacionadas:

- [OPS02-BP02 Processos e procedimentos com proprietários identificados](#): os processos e procedimentos para apoiar os recursos dependem do proprietário do recurso.
- [OPS02-BP04 Os membros da equipe sabem pelo que são responsáveis](#): os membros da equipe devem saber de quais recursos eles são proprietários.
- [OPS02-BP05 Existem mecanismos para identificar a responsabilidade e a propriedade](#): é necessário usar mecanismos como tags e contatos de conta para que a propriedade possa ser descoberta.

Documentos relacionados:

- [AWS Account Management: Atualizar informações de contato](#)
- [Regras do AWS Config: required-tags](#)
- [AWS Organizations: Atualizar contatos alternativos em sua organização](#)
- [Whitepaper Práticas recomendadas de marcação AWS](#)

Exemplos relacionados:

- [Regras do AWS Config: Amazon EC2 com regras requeridas e valores válidos](#)

Serviços relacionados:

- [AWS Config](#)

- [AWS Organizations](#)

OPS02-BP02 Processos e procedimentos com proprietários identificados

Entenda quem tem a propriedade da definição de processos e procedimentos individuais, por que esses processos e procedimentos específicos são usados e por que essa propriedade existe. Entender os motivos pelos quais processos e procedimentos específicos são usados permite identificar oportunidades de melhoria.

Benefícios do estabelecimento desta prática recomendada: Entender a propriedade identifica quem pode aprovar melhorias, implementar essas melhorias ou ambos.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Alto

Orientações para a implementação

- Processos e procedimentos com proprietários identificados responsáveis pela sua definição: capture os processos e procedimentos usados em seu ambiente e o indivíduo ou a equipe responsável pela sua definição.
 - Identifique processos e procedimentos: identifique as atividades de operações realizadas para dar suporte às suas workloads. Documente essas atividades em um local que possa ser localizado.
 - Defina quem é o proprietário de um processo ou procedimento: identifique exclusivamente o indivíduo ou a equipe responsável pela especificação de uma atividade. Eles são responsáveis por garantir que ela possa ser executada com êxito por um membro da equipe devidamente qualificado com as permissões, as ferramentas e o acesso corretos. Se houver problemas com a execução dessa atividade, os membros da equipe que a executam serão responsáveis por fornecer os comentários detalhados necessários para que a atividade seja melhorada.
 - Capture a propriedade de artefato de atividades nos metadados: os procedimentos automatizados em serviços como o AWS Systems Manager, por meio de documentos, e o AWS Lambda, como funções, são compatíveis com a captura de informações de metadados como tags. Capture a propriedade de recursos usando tags ou grupos de recursos, especificando propriedade e informações de contato. Use o AWS Organizations para criar políticas de marcação e garantir que as informações de propriedade e de contato sejam capturadas.

OPS02-BP03 Atividades de operações com proprietários identificados responsáveis pela performance

Entenda quem tem a responsabilidade de realizar atividades específicas em cargas de trabalho definidas e por que essa responsabilidade existe. Entender quem tem a responsabilidade de realizar atividades informa quem realizará a atividade, validará o resultado e fornecerá feedback ao proprietário da atividade.

Benefícios do estabelecimento desta prática recomendada: Entender quem é responsável por realizar uma atividade informa a quem notificar quando uma ação é necessária e quem executará a ação, validará o resultado e fornecerá feedback ao proprietário da atividade.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Alto

Orientações para a implementação

- Atividades de operações com proprietários identificados responsáveis por sua performance: capture a responsabilidade por executar processos e procedimentos usados em seu ambiente.
 - Identificar processos e procedimentos: identifique as atividades de operações realizadas para dar suporte às suas workloads. Documente essas atividades em um local que possa ser localizado.
 - Definir quem é responsável por executar cada atividade: identifique a equipe responsável por uma atividade. Certifique-se de que eles tenham os detalhes da atividade e as habilidades necessárias e as permissões, as ferramentas e o acesso corretos para realizar a atividade. Eles devem compreender a condição sob a qual ela deve ser executada (por exemplo, em um evento ou programação). Torne essas informações detectáveis para que os membros da sua organização possam identificar com quem precisam entrar em contato, equipe ou indivíduo, para necessidades específicas.

OPS02-BP04 Os membros da equipe sabem pelo que são responsáveis

Entender as responsabilidades de sua função e como você contribui para resultados comerciais informa a priorização de suas tarefas e por que sua função é importante. Isso permite que os membros da equipe reconheçam as necessidades e respondam adequadamente.

Benefícios do estabelecimento desta prática recomendada: entender suas responsabilidades fundamenta as decisões que você toma, as ações que você realiza e suas atividades de entrega aos proprietários apropriados.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

- Garantir que os membros da equipe compreendam suas funções e responsabilidades: identifique as funções e responsabilidades dos membros da equipe e garanta que eles compreendam as expectativas da função que exercem. Torne essas informações detectáveis para que os membros da sua organização possam identificar com quem precisam entrar em contato, equipe ou indivíduo, para necessidades específicas.

OPS02-BP05 Existem mecanismos para identificar a responsabilidade e a propriedade

Quando nenhum indivíduo ou equipe é identificado, há caminhos de escalonamento definidos para alguém com autoridade para atribuir propriedade ou plano para o que precisa ser abordado.

Benefícios do estabelecimento desta prática recomendada: Entender quem tem responsabilidade ou propriedade permite que você entre em contato com a equipe ou o membro da equipe apropriado para fazer uma solicitação ou a transição de uma tarefa. Ter uma pessoa identificada que tenha a autoridade para atribuir responsabilidade ou propriedade ou planejar atender às necessidades, reduz o risco de inação, além de não ser preciso lidar com isso.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Alto

Orientações para a implementação

- Mecanismos existentes para identificar a responsabilidade e a propriedade: forneça mecanismos acessíveis para que os membros da sua organização descubram e identifiquem a propriedade e a responsabilidade. Esses mecanismos permitirão que eles identifiquem com quem entrar em contato, equipe ou indivíduo, em caso de necessidades específicas.

OPS02-BP06 Mecanismos existem para solicitar adições, alterações e exceções

Você pode fazer solicitações aos proprietários de processos, procedimentos e recursos. Solicitações incluem adições, alterações e exceções. Essas solicitações passam por um processo de gerenciamento de alterações. Tome decisões embasadas para aprovar solicitações quando elas forem viáveis e foram consideradas apropriadas após uma avaliação de benefícios e riscos.

Resultado desejado:

- Você pode fazer solicitações para alterar processos, procedimentos e recursos com base na propriedade atribuída.
- As alterações são feitas de maneira deliberada, ponderando benefícios e riscos.

Antipadrões comuns:

- Você precisa atualizar a maneira como implanta sua aplicação, mas não há como solicitar uma alteração no processo de implantação à equipe de operações.
- O plano de recuperação de desastres deve ser atualizado, mas não há nenhum proprietário identificado para solicitar alterações no plano.

Benefícios do estabelecimento desta prática recomendada:

- Processos, procedimentos e recursos podem evoluir à medida que os requisitos mudam.
- Os proprietários podem tomar decisões embasadas sobre quando realizar alterações.
- As alterações são feitas de maneira deliberada.

Nível de risco exposto se esta prática recomendada não é estabelecida: médio

Orientações para a implementação

Para implementar esta prática recomendada, você precisa estar em uma posição em que possa solicitar alterações em processos, procedimentos e recursos. O processo de gerenciamento de alterações pode ser simples. Documente o processo de gerenciamento de alterações.

Exemplo de clientes

A Loja UmaEmpresa usa a matriz de atribuição de responsabilidades (RACI) para identificar quem é proprietário das alterações em processos, procedimentos e recursos. Eles documentaram o processo de gerenciamento de alterações, que é simples e fácil de seguir. Usando a matriz RACI e o processo, qualquer pessoa pode enviar solicitações de alteração.

Etapas da implementação

1. Identifique processos, procedimentos e recursos para sua workload e os proprietários de cada um. Documente-os no sistema de gerenciamento de conhecimentos.
 - a. Se você não tiver implementado [OPS02-BP01 Recursos com proprietários identificados](#), [OPS02-BP02 Processos e procedimentos com proprietários identificados](#) ou [OPS02-BP03](#)

[Atividades de operações com proprietários identificados responsáveis pela performance](#), comece com estes.

2. Trabalhe com as partes interessadas em sua organização para desenvolver um processo de gerenciamento de alterações. O processo deve abranger adições, alterações e exceções para recursos, processos e procedimentos.
 - a. Você pode usar o [Gerente de Alterações do AWS Systems Manager](#) como plataforma de gerenciamento de alterações para recursos de workload.
3. Documente o processo de gerenciamento de alterações em seu sistema de gerenciamento de conhecimentos.

Nível de esforço do plano de implementação: médio. O desenvolvimento de um processo de gerenciamento de alterações deve estar alinhado com várias partes interessadas em sua organização.

Recursos

Práticas recomendadas relacionadas:

- [OPS02-BP01 Recursos com proprietários identificados](#): para criar um processo de gerenciamento de alterações, primeiro é necessário identificar os proprietários dos recursos.
- [OPS02-BP02 Processos e procedimentos com proprietários identificados](#): para criar um processo de gerenciamento de alterações, primeiro é necessário identificar os proprietários dos recursos.
- [OPS02-BP03 Atividades de operações com proprietários identificados responsáveis pela performance](#): para criar um processo de gerenciamento de alterações, primeiro é necessário identificar os proprietários.

Documentos relacionados:

- [AWS Prescriptive Guidance - Foundation playbook for AWS large migrations: Creating RACI matrices](#)
- [Whitepaper Gerenciamento de alterações na nuvem](#)

Serviços relacionados:

- [Gerente de Alterações do AWS Systems Manager](#)

OPS02-BP07 As responsabilidades entre as equipes são predefinidas ou negociadas

Tenha acordos definidos ou negociados entre as equipes que descrevam como elas trabalham e oferecem suporte umas às outras (por exemplo, tempos de resposta, objetivos de nível de serviço ou Acordos de Serviço). Os canais de comunicação entre equipes são documentados. Ao entender o impacto do trabalho das equipes nos resultados de negócios e nos resultados de outras equipes e organizações, você conhece a priorização de tarefas delas e as ajuda a responder adequadamente.

Quando a responsabilidade e a propriedade não foram definidas ou são desconhecidas, você corre o risco de não abordar as atividades necessárias em tempo hábil e de despender esforços redundantes e possivelmente conflitantes para atender a essas necessidades.

Resultado desejado:

- Os acordos de trabalho ou apoio entre equipes são combinados e documentados.
- As equipes que apoiam ou trabalham umas com as outras definiram canais de comunicação e expectativas de resposta.

Antipadrões comuns:

- Ocorre um problema na produção e duas equipes separadas começam a resolução de problemas de maneira independente. Esses esforços isolados estendem a interrupção.
- A equipe de operações necessita de assistência da equipe de desenvolvimento, mas nenhum tempo de resposta foi acordado. A solicitação está parada em uma lista de pendências.

Benefícios do estabelecimento desta prática recomendada:

- As equipes sabem interagir e apoiar uma à outra.
- As expectativas quanto à capacidade de resposta são claras.
- Os canais de comunicação estão nitidamente definidos.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: baixo

Orientações para a implementação

A implementação desta prática recomendada significa que não há ambiguidade quanto à forma como as equipes trabalham uma com a outra. Os acordos formais sistematizam de que maneira as

equipes trabalham juntas ou apoiam uma à outra. Os canais de comunicação entre as equipes são documentados.

Exemplo de clientes

A equipe de SRE da Loja UmaEmpresa tem um Acordo de Serviço com a equipe de desenvolvimento. Sempre que a equipe de desenvolvimento faz uma solicitação no sistema de tíquetes, ela pode esperar uma resposta em 15 minutos. Se não houver nenhuma interrupção no local, a equipe de SRE toma a dianteira na investigação e conta com o apoio da equipe de desenvolvimento.

Etapas da implementação

1. Trabalhando com as partes interessadas na organização, desenvolva acordos entre as equipes com base nos processos e procedimentos.
 - a. Se um processo ou procedimento for compartilhado entre as duas equipes, desenvolva um runbook sobre como as equipes trabalharão juntas.
 - b. Se houver dependências entre as equipes, estabeleça um SLA de resposta às solicitações.
2. Documente as responsabilidades no sistema de gerenciamento de conhecimentos.

Nível de esforço do plano de implementação: médio. Se não houver nenhum entendimento entre as equipes, pode ser difícil chegar a um acordo com as partes interessadas na organização.

Recursos

Práticas recomendadas relacionadas:

- [OPS02-BP02 Processos e procedimentos com proprietários identificados](#): para estabelecer acordos entre as equipes, primeiro é necessário identificar o proprietário do processo.
- [OPS02-BP03 Atividades de operações com proprietários identificados responsáveis pela performance](#): para estabelecer acordos entre as equipes, primeiro é necessário identificar o proprietário das atividades de operações.

Documentos relacionados:

- [AWS Executive Insights: Impulsionando inovação e velocidade com as equipes de duas pizzas da Amazon](#)
- [Introdução a DevOps na AWS: Equipes de duas pizzas](#)

Cultura organizacional

Forneça suporte aos membros da equipe, para que eles possam ser mais eficazes na hora de tomar medidas e colaborar com os resultados de negócios.

Práticas recomendadas

- [OPS03-BP01 Patrocínio executivo](#)
- [OPS03-BP02 Os membros da equipe estão capacitados para executar ações quando os resultados estão em risco.](#)
- [OPS03-BP03 Incentivo ao escalonamento](#)
- [OPS03-BP04 Comunicações oportunas, claras e acionáveis](#)
- [OPS03-BP05 Incentivo à experimentação](#)
- [OPS03-BP06 Os membros da equipe estão capacitados e são incentivados a manter e a aumentar seus conjuntos de habilidades.](#)
- [OPS03-BP07 Fornecer recursos adequados às equipes](#)
- [OPS03-BP08 Opiniões diversas são incentivadas e procuradas dentro e entre equipes](#)

OPS03-BP01 Patrocínio executivo

A liderança sênior define claramente as expectativas para a organização e avalia o êxito. A liderança sênior é patrocinadora, defensora e motivadora da adoção das melhores práticas e da evolução da organização

Benefícios do estabelecimento desta prática recomendada: A liderança engajada, as expectativas comunicadas claramente e as metas compartilhadas garantem que os membros da equipe saibam o que se espera deles. A avaliação do sucesso possibilita a identificação de barreiras para o sucesso, para que elas possam ser abordadas por meio da intervenção do patrocinador ou dos representantes dele.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Alto

Orientações para a implementação

- Patrocínio executivo: a liderança sênior define claramente as expectativas para a organização e avalia o êxito. A liderança sênior é patrocinadora, defensora e motivadora da adoção das melhores práticas e da evolução da organização

- Definir as expectativas: defina e publique metas para suas organizações, incluindo como elas serão medidas.
- Monitorar a concretização das metas: meça regularmente a concretização incremental das metas e compartilhe os resultados para que medidas adequadas possam ser tomadas se os resultados estiverem em risco.
- Fornecer os recursos necessários para realizar suas metas: analise regularmente se os recursos ainda são apropriados ou se recursos adicionais são necessários com base em novas informações, alterações nas metas, responsabilidades ou ambiente da empresa.
- Defender suas equipes: mantenha o envolvimento com suas equipes para compreender a performance delas e se estão sendo afetadas por fatores externos. Quando suas equipes forem afetadas por fatores externos, reavalie metas e ajuste os objetivos conforme apropriado. Identifique os obstáculos que estão impedindo o progresso das suas equipes. Aja em nome das suas equipes para ajudar a resolver obstáculos e eliminar obrigações desnecessárias.
- Motivar a adoção de práticas recomendadas: confirme as práticas recomendadas que oferecem benefícios quantificáveis e reconheça quem as cria e as adota. Incentive ainda mais a adoção para ampliar os benefícios obtidos.
- Motivar a evolução de suas equipes: crie uma cultura de melhoria contínua. Incentive o crescimento e o desenvolvimento pessoal e organizacional. Forneça metas de longo prazo pelas quais se esforçar que exigirão conquistas incrementais ao longo do tempo. Ajuste essa visão para complementar necessidades, metas de negócios e ambiente de negócios à medida que eles mudarem.

OPS03-BP02 Os membros da equipe estão capacitados para executar ações quando os resultados estão em risco.

O proprietário da carga de trabalho definiu orientação e escopo, permitindo que os membros da equipe respondam quando os resultados estiverem em risco. Mecanismos de escalonamento são usados para obter orientação quando os eventos estão fora do escopo definido.

Benefícios do estabelecimento desta prática recomendada: Ao testar e validar alterações antecipadamente, você pode resolver problemas com custos reduzidos e limitar o impacto sobre seus clientes. Ao testar antes da implantação, você reduz a possibilidade de erros.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Alto

Orientações para a implementação

- Os membros da equipe estão capacitados para executar ações quando os resultados estão em risco: forneça aos membros da equipe as permissões, as ferramentas e a oportunidade de praticar as habilidades necessárias para responderem com eficácia.
 - Fornecer aos membros da equipe a oportunidade de praticar as habilidades necessárias para responder: forneça ambientes alternativos e seguros em que os processos e os procedimentos possam ser testados e treinados com segurança. Realizar dias de jogos para permitir que os membros da equipe adquiram experiência para responder a incidentes reais em ambientes simulados e seguros.
 - Definir e confirmar a autoridade dos membros da equipe para executar ações: defina especificamente a autoridade dos membros da equipe para executar ações por meio da atribuição de permissões e acesso às workloads e aos componentes aos quais oferecem suporte. Reconheça que eles estão capacitados a executar ações quando os resultados estão em risco.

OPS03-BP03 Incentivo ao escalonamento

Os membros da equipe têm mecanismos e são incentivados a escalar as preocupações para os tomadores de decisão e as partes interessadas se acharem que os resultados estão em risco. O escalonamento deve ser realizado de maneira antecipada e frequente para que os riscos possam ser identificados e isso evite incidentes.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Alto

Orientações para a implementação

- Incentivar o escalonamento antecipado e frequente: reconheça de forma organizacional que o escalonamento antecipado e frequente é a prática recomendada. Reconheça e aceite de maneira organizacional que os escalonamentos podem ser infundados e que é melhor ter a oportunidade de evitar um incidente do que perder essa oportunidade ao não escalar.
- Ter um mecanismo para o escalonamento: tenha procedimentos documentados que definem quando e como o escalonamento deve ocorrer. Documente a série de pessoas com autoridade crescente para tomar medidas ou aprovar ações e as informações de contato delas. O escalonamento deve continuar até que o membro da equipe esteja satisfeito por ter transmitido o risco a alguém capaz de lidar com ele ou tenha entrado em contato com a pessoa que detém o risco e a responsabilidade pela operação da workload. É essa pessoa que, em última análise,

tem todas as decisões com relação à carga de trabalho. Os escalonamentos devem incluir a natureza do risco, a criticidade da carga de trabalho, quem é afetado, qual é o impacto e a urgência, ou seja, quando é o impacto esperado.

- Proteger os funcionários que usam o escalonamento: tenha uma política que proteja os membros da equipe contra retaliações se fizerem um escalonamento em relação a um tomador de decisão ou parte interessada não responsivo. Tenha mecanismos implementados para identificar se isso está ocorrendo e responder de maneira adequada.

OPS03-BP04 Comunicações oportunas, claras e acionáveis

Mecanismos existem e são usados para fornecer avisos oportunos aos membros da equipe acerca de riscos conhecidos e eventos planejados. Contexto, detalhes e tempo necessários (quando possível) são fornecidos para ajudar a determinar se há necessidade de uma ação e qual ação é necessária e a tomar as medidas necessárias em tempo hábil. Por exemplo, a notificação de vulnerabilidades de software para que a aplicação de patches possa ser expressa ou o aviso de promoções de vendas planejadas para que um congelamento de alterações possa ser implementado para evitar o risco de interrupção do serviço. Eventos planejados podem ser registrados em um calendário de alterações ou programação de manutenção para que os membros da equipe possam identificar quais atividades estão pendentes.

Resultado desejado:

- A comunicação fornece contexto, detalhes e expectativas de tempo.
- Os membros da equipe têm um entendimento claro sobre quando e como agir em resposta a comunicações.
- Utilize calendários de alterações para chamar a atenção para as alterações previstas.

Antipadrões comuns:

- Um alerta falso-positivo é acionado várias vezes por semana. Você silencia a notificação toda vez em que ela ocorre.
- Você recebe uma solicitação para alterar seu grupo de segurança, mas não é passada nenhuma expectativa sobre quando isso deve ocorrer.
- Você recebe notificações constantes por chat quando a escala dos sistemas é aumentada verticalmente, mas nenhuma ação é necessária. Você evita o canal por chat e perde uma notificação importante.

- Fizeram uma alteração na produção sem informar a equipe de operações. A alteração aciona um alerta e a equipe de plantão é ativada.

Benefícios do estabelecimento desta prática recomendada:

- Sua organização evita a fadiga de alertas.
- Os membros da equipe podem agir com o contexto necessário e as expectativas indispensáveis.
- As alterações podem ser feitas durante períodos apropriados e reduzir o risco.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

Para implementar esta prática recomendada, você precisa trabalhar com as partes interessadas na organização para ajustar padrões de comunicação. Divulgue esses padrões para toda a organização. Identifique e remova alertas falso-positivos ou que fiquem sempre ativos. Utilize calendários de alterações para que os membros da equipe saibam quando é possível agir e quais atividades estão pendentes. Verifique se as comunicações geram ações claras com o contexto necessário.

Exemplo de clientes

A Loja UmaEmpresa usa o chat como principal meio de comunicação. Alertas e outras informações são divulgados em canais específicos. Quando alguém precisa agir, o resultado desejado é claramente expresso, e, em muitos casos, as pessoas recebem um runbook ou manual para uso nessas situações. O calendário de alterações é usado para programar alterações importantes nos sistemas de produção.

Etapas da implementação

1. Analise os alertas para identificar falso-positivos ou alertas que são acionados constantemente. Remova ou altere esses alertas para que sejam acionados quando há necessidade de intervenção humana. Se um alerta for acionado, forneça um runbook ou manual.
 - a. Você pode usar [Documentos do AWS Systems Manager](#) para criar manuais e runbooks para alertas.
2. Mecanismos estão em vigor para fornecer notificações de riscos ou eventos planejados de maneira clara e prática com aviso prévio em tempo suficiente para permitir respostas apropriadas. Use listas de e-mails ou canais por chat para enviar notificações antes dos eventos planejados.

- a. [É possível usar o AWS Chatbot](#) para enviar alertas e responder a eventos dentro da plataforma de mensagens de suas organizações.
3. Forneça uma fonte de informações acessível em que eventos planejados possam ser descobertos. Forneça notificações de eventos planejados oriundos do mesmo sistema.
 - a. [O Calendário de Alterações do AWS Systems Manager](#) pode ser usado para criar períodos em que as alterações podem ocorrer. Isso oferece aos membros da equipe um aviso prévio sobre quando eles podem fazer alterações com segurança.
4. Monitore notificações de vulnerabilidade e informações de patches para identificar vulnerabilidades nos riscos reais e potenciais associados aos componentes da workload. Forneça uma notificação aos membros da equipe para que eles possam agir.
 - a. Você pode assinar os [boletins de segurança da AWS](#) para receber notificações sobre vulnerabilidades na AWS.

Recursos

Práticas recomendadas relacionadas:

- [OPS07-BP03 Usar runbooks para realizar procedimentos](#): para que as comunicações tenham efeito prático, forneça um runbook quando o resultado for conhecido.
- [OPS07-BP04 Usar manuais para investigar problemas](#): quando não se conhece o resultado, os manuais podem tornar as comunicações acionáveis.

Documentos relacionados:

- [Boletins de segurança da AWS](#)
- [Open CVE](#)

Exemplos relacionados:

- [Laboratórios do Well-Architected: Gerenciamento de inventário e patches \(Nível 100\)](#)

Serviços relacionados:

- [AWS Chatbot](#)
- [Calendário de alterações do AWS Systems Manager](#)

- [Documentos do AWS Systems Manager](#)

OPS03-BP05 Incentivo à experimentação

A experimentação é um catalisador para transformar novas ideias em produtos e recursos. Ela acelera o aprendizado e mantém os membros da equipe interessados e envolvidos. Os membros da equipe são incentivados a experimentar com frequência para promover a inovação. Mesmo quando um resultado não desejado ocorre, é importante saber o que não se deve fazer. Os membros da equipe não são punidos por experimentos bem-sucedidos com resultados indesejados.

Resultado desejado:

- Sua organização incentiva a experimentação para promover a inovação.
- Os experimentos são usados como oportunidade de aprendizado.

Antipadrões comuns:

- Você deseja executar um teste A/B, mas não há nenhum mecanismo para conduzir o experimento. Você implanta uma alteração de interface do usuário sem a possibilidade de testá-la. O resultado é uma experiência negativa para o cliente.
- Sua empresa tem apenas o ambiente de preparação e produção. Como não há área restrita para testes para experimentar novos recursos ou produtos, você precisa realizar experimentos no ambiente de produção.

Benefícios do estabelecimento desta prática recomendada:

- A experimentação promove a inovação.
- Você reagir mais depressa ao feedback dos usuários por meio da experimentação.
- Sua organização desenvolve uma cultura de aprendizado.

Nível de risco exposto se esta prática recomendada não é estabelecida: médio

Orientações para a implementação

Os experimentos devem ser conduzidos de maneira segura. Utilize vários ambientes para experimentar, sem colocar em risco os recursos da produção. Use testes A/B e sinalizadores de

recursos para testar experimentos. Ofereça aos membros da equipe a possibilidade de conduzir experimentos em um ambiente de área restrita para testes.

Exemplo de clientes

A Loja UmaEmpresa estimula a experimentação. Os membros da equipe podem usar 20% da semana de trabalho para experimentar ou aprender novas tecnologias. Eles têm um ambiente de área restrita para testes no qual podem inovar. São usados testes A/B para novos recursos com o objetivo de validá-los com um feedback de usuário real.

Etapas da implementação

1. Trabalhe com a liderança em toda a sua organização para favorecer a experimentação. Os membros da equipe devem ser incentivados a conduzir experimentos de maneira segura.
2. Ofereça aos membros da equipe um ambiente em que eles possa experimentar com segurança. Eles devem ter acesso a um ambiente semelhante ao de produção.
 - a. Você pode usar uma Conta da AWS separada para criar um ambiente de área restrita para testes para experimentação. O [AWS Control Tower](#) pode ser usado para provisionar essas contas.
3. Use sinalizadores de recursos e testes A/B para experimentar com segurança e coletar feedback dos usuários.
 - a. O [AWS AppConfig](#) Feature Flags oferece a possibilidade de criar sinalizadores de recursos.
 - b. O [Amazon CloudWatch Evidently](#) pode ser usado para realizar testes A/B em uma implantação limitada.
 - c. Você pode usar [versões do AWS Lambda](#) para implantar uma nova versão de uma função para testes beta.

Nível de esforço do plano de implementação: alto. A viabilização de um ambiente para experimentação e de uma maneira segura para os membros da equipe conduzirem experimentos pode exigir um investimento significativo. Você também pode precisar modificar o código da aplicação para usar sinalizadores de recursos ou respaldar testes A/B.

Recursos

Práticas recomendadas relacionadas:

- [OPS11-BP02 Executar análise pós-incidente](#): aprender com incidentes é um motivador fundamental para a inovação, bem como a experimentação.

- [OPS11-BP03 Implementar loops de feedback](#): os ciclos de feedback são um componente importante da experimentação.

Documentos relacionados:

- [Uma visão interna da cultura da Amazon: experimentação, erro e obsessão pelo cliente](#)
- [Práticas recomendadas para criar e gerenciar contas em área restrita para testes na AWS](#)
- [Crie uma cultura de experimentação viabilizada pela nuvem](#)
- [Viabilização da experimentação e inovação na nuvem na SulAmérica Seguros](#)
- [Experimente mais, erre menos](#)
- [Organização do ambiente da AWS usando várias contas: UO de área restrita para testes](#)
- [Como usar o AWS AppConfig Feature Flags](#)

Vídeos relacionados:

- [AWS On Air ft. Amazon CloudWatch Evidently | AWS Eventos](#)
- [AWS On Air San Fran Summit 2022 ft. Integração do AWS AppConfig Feature Flags com o Jira](#)
- [AWS re:Invent 2022: Implantação não é lançamento: controle seus lançamentos com sinalizadores de recursos \(BOA305-R\)](#)
- [Crie programaticamente uma Conta da AWS com o AWS Control Tower](#)
- [Configuração de um ambiente de várias contas da AWS que usa as práticas recomendadas para AWS Organizations](#)

Exemplos relacionados:

- [AWS Innovation Sandbox](#)
- [Personalização básica de ponta a ponta para comércio eletrônico](#)

Serviços relacionados:

- [Amazon CloudWatch Evidently](#)
- [AWS AppConfig](#)
- [AWS Control Tower](#)

OPS03-BP06 Os membros da equipe estão capacitados e são incentivados a manter e a aumentar seus conjuntos de habilidades.

As equipes devem aumentar os conjuntos de habilidades para adotar novas tecnologias e apoiar mudanças na demanda e responsabilidades no apoio às suas cargas de trabalho. O desenvolvimento das habilidades em novas tecnologias costuma ser uma fonte de satisfação dos membros da equipe e apoia a inovação. Ofereça apoio aos membros da equipe na busca e atualização de certificações do setor que validem e reconheçam as suas habilidades crescentes. Treine profissionais em diferentes funções para promover a transferência de conhecimento e reduzir o risco de impacto significativo quando você perde membros da equipe qualificados e experientes com conhecimento institucional. Reserve tempo estruturado e dedicado para o aprendizado.

A AWS fornece recursos, incluindo o [Centro de recursos de conceitos básicos da AWS](#), [Blogs da AWS](#), [AWS Online Tech Talks](#), [Eventos e webinars da AWS](#) e os [Laboratórios do AWS Well-Architected](#), que fornecem orientações, exemplos e demonstrações detalhadas para educar suas equipes.

A AWS também compartilha as práticas recomendadas e os padrões que aprendemos durante a operação da AWS na [Amazon Builders' Library](#) e uma grande variedade de outros materiais educacionais úteis por meio do [Blog da AWS](#) e [O podcast oficial da AWS](#).

Você deve aproveitar os recursos educacionais fornecidos pela AWS, como os laboratórios do AWS Well-Architected, [AWS Support](#) ([Centro de Conhecimentos da AWS](#), [Fóruns de discussão da AWS](#) e aos [AWS Support Center](#)) e [Documentação da AWS](#) para instruir suas equipes. Entre em contato com o AWS Support por meio do AWS Support Center para obter ajuda com relação às suas dúvidas sobre a AWS.

[Treinamento da AWS and Certification](#) fornece alguns treinamentos gratuitos por meio de cursos digitais autoguiados sobre os conceitos básicos da AWS. Também é possível inscrever-se em treinamento administrado por instrutor para oferecer suporte adicional ao desenvolvimento das habilidades em AWS de suas equipes.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Médio

Orientações para a implementação

- Os membros da equipe estão capacitados e são incentivados a manter e a ampliar seus conjuntos de habilidades: para adotar novas tecnologias e oferecer suporte às mudanças na demanda e nas responsabilidades de suporte às workloads, é necessário treinamento contínuo.

- Fornecer recursos para treinamento: forneça tempo estruturado dedicado, acesso ao material de treinamento, recursos de laboratório e suporte à participação em conferências e organizações profissionais que fornecem oportunidades para aprendizado para instrutores e colegas. Forneça aos membros da equipe júnior acesso aos membros da equipe sênior como mentores ou permita que eles sigam o trabalho deles e sejam expostos aos métodos e às habilidades que têm. Incentive o aprendizado sobre conteúdo não diretamente relacionado ao trabalho para ter uma perspectiva mais ampla.
- Treinamento da equipe e envolvimento entre equipes: planeje as necessidades de treinamento contínuo dos membros da equipe. Ofereça oportunidades para que os membros da equipe se juntem a outras equipes (temporária ou permanentemente) para compartilhar habilidades e melhores práticas que beneficiam toda a organização
- Oferecer suporte à busca e à manutenção de certificações do setor: ofereça suporte à aquisição e manutenção de certificações do setor que validam o aprendizado e reconheça as conquistas dos membros da equipe.

Recursos

Documentos relacionados:

- [Centro de recursos de conceitos básicos da AWS](#)
- [Blogs da AWS](#)
- [Conformidade da Nuvem AWS](#)
- [Fóruns de discussão da AWS](#)
- [Documentação da AWS](#)
- [AWS Online Tech Talks](#)
- [Eventos e webinars da AWS](#)
- [Centro de Conhecimentos da AWS](#)
- [AWS Support](#)
- [Treinamento da AWS and Certification](#)
- [Laboratórios do AWS Well-Architected,](#)
- [Amazon Builders' Library](#)
- [O podcast oficial da AWS.](#)

OPS03-BP07 Fornecer recursos adequados às equipes

Mantenha a capacidade dos membros da equipe e forneça ferramentas e recursos para dar suporte às necessidades da workload. A sobrecarga de membros da equipe aumenta o risco de incidentes resultantes de erros humanos. Os investimentos em ferramentas e em recursos (por exemplo, o fornecimento de automação para atividades executadas com frequência) podem escalar a eficácia da equipe, permitindo que ela ofereça suporte a atividades adicionais.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

- Fornecer recursos adequados às equipes: compreenda o sucesso das equipes e os fatores que contribuem para o sucesso ou para o insucesso. Aja para apoiar equipes com os recursos apropriados.
 - Compreender a performance da equipe: meça a aquisição de resultados operacionais e o desenvolvimento de ativos realizados pela equipe. Acompanhe as alterações na saída e na taxa de erros ao longo do tempo. Envolver-se com as equipes para compreender os desafios relacionados ao trabalho que as afetam (por exemplo, aumento de responsabilidades, mudanças na tecnologia, perda de pessoal ou aumento de clientes atendidos pelo suporte).
 - Compreender os impactos na performance das equipes: mantenha-se engajado com as equipes para entender como elas estão desempenhando e se há fatores externos que as afetam. Quando suas equipes forem afetadas por fatores externos, reavalie metas e ajuste os objetivos conforme apropriado. Identifique os obstáculos que estão impedindo o progresso das suas equipes. Aja em nome das suas equipes para ajudar a resolver obstáculos e eliminar obrigações desnecessárias.
 - Fornecer os recursos necessários para as equipes serem bem-sucedidas: analise regularmente se os recursos ainda são adequados, ou se são necessários recursos adicionais, e faça os ajustes apropriados para oferecer suporte às equipes.

OPS03-BP08 Opiniões diversas são incentivadas e procuradas dentro e entre equipes

Aproveite a diversidade entre organizações para buscar várias perspectivas únicas. Use essa abordagem para aumentar a inovação, desafiar suas suposições e reduzir o risco de viés de confirmação. Aumente a inclusão, a diversidade e a acessibilidade em suas equipes para obter perspectivas benéficas.

A cultura organizacional tem impacto direto na satisfação com a tarefa e na retenção dos membros da equipe. Incentive o envolvimento e as habilidades dos membros da equipe para promover o êxito da sua empresa.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Baixo

Orientações para a implementação

- Buscar opiniões e perspectivas diversas: incentive contribuições de todos. Ouça os grupos de pequena representação. Alterne as funções e as responsabilidades em reuniões.
- Expandir funções e responsabilidades: ofereça oportunidade para que os membros da equipe assumam funções que não poderiam assumir de outra forma. Eles ganharão experiência e perspectiva com a função e com as interações com novos membros da equipe com os quais não interagiriam de outra forma. Eles levarão a experiência e perspectiva deles para a nova função e para os membros da equipe com os quais interagirem. Conforme aumenta a perspectiva, mais oportunidades de negócios podem surgir ou novas oportunidades de melhoria podem ser identificadas. Faça com que os membros de uma equipe se revezem em tarefas comuns que outras pessoas normalmente executam para compreender as demandas e o impacto de realizá-las.
- Fornecer um ambiente seguro e acolhedor: implante políticas e controles que protejam a segurança física e mental dos membros da equipe na organização. Os membros da equipe devem poder interagir sem medo de represálias. Quando os membros da equipe se sentem seguros e bem-vindos, eles provavelmente estão envolvidos e são produtivos. Quanto mais diversificada sua organização, melhor será o entendimento das pessoas que você apoia, incluindo seus clientes. Quando os membros da equipe estiverem confortáveis, sentirem-se à vontade para falar e confiarem que serão ouvidos, será mais provável que eles dividam ideias valiosas (por exemplo, oportunidades de marketing, necessidades de acessibilidade, segmentos de mercado não atendidos, riscos não reconhecidos no seu ambiente).
- Permitir que os membros da equipe participem plenamente: forneça os recursos necessários para que os funcionários participem totalmente de todas as atividades relacionadas ao trabalho. Os membros da equipe que enfrentam desafios diários desenvolveram habilidades para contornar esses desafios. Essas habilidades desenvolvidas exclusivamente podem oferecer benefícios significativos para a sua organização. O apoio aos membros da equipe com as acomodações necessárias aumentará os benefícios que você poderá receber das contribuições deles.

Preparar

Para se preparar para a excelência operacional, você precisa entender suas workloads e os comportamentos esperados. Você poderá projetá-las para fornecer insights sobre seu status e criar os procedimentos para oferecer suporte a elas.

Para se preparar para a excelência operacional, é necessário considerar o seguinte:

Tópicos

- [Implementar a observabilidade](#)
- [Design das operações](#)
- [Mitigar riscos de implantação](#)
- [Prontidão operacional e gerenciamento de alterações](#)

Implementar a observabilidade

Implemente a observabilidade na workload para que você possa entender seu estado e tomar decisões baseadas em dados com base nos requisitos de negócios.

A observabilidade vai além do simples monitoramento, fornecendo uma compreensão abrangente do funcionamento interno de um sistema com base em suas saídas externas. Baseada em métricas, logs e rastreamentos, a observabilidade oferece insights profundos sobre o comportamento e a dinâmica do sistema. Com uma observabilidade eficaz, as equipes podem discernir padrões, anomalias e tendências, permitindo que abordem proativamente possíveis problemas e mantenham a integridade ideal do sistema.

Identificar os indicadores-chave de performance (KPIs) é fundamental para garantir o alinhamento entre as atividades de monitoramento e os objetivos de negócios. Esse alinhamento garante que as equipes tomem decisões baseadas em dados usando métricas que realmente importam, otimizando o desempenho do sistema e os resultados comerciais.

Além disso, a observabilidade capacita as empresas a serem proativas em vez de reativas. As equipes podem entender as relações de causa e efeito em seus sistemas, prevendo e prevenindo problemas em vez de apenas reagir a eles. À medida que as workloads evoluem, é essencial revisar e refinar a estratégia de observabilidade, garantindo que ela permaneça relevante e eficaz.

Práticas recomendadas

- [OPS04-BP01 Identificar os indicadores-chave de performance](#)
- [OPS04-BP02 Implementar a telemetria de aplicações](#)
- [OPS04-BP03 Implementar a telemetria da experiência do usuário](#)
- [OPS04-BP04 Implementar a telemetria de dependências](#)
- [OPS04-BP05 Implementar rastreamento distribuído](#)

OPS04-BP01 Identificar os indicadores-chave de performance

A implementação da observabilidade em sua workload começa com a compreensão de seu estado e a tomada de decisões baseadas em dados conforme os requisitos de negócios. Uma das formas mais eficazes de garantir o alinhamento entre as atividades de monitoramento e os objetivos de negócios é definir e monitorar os indicadores-chave de performance (KPIs).

Resultado desejado: Práticas de observabilidade eficientes que estão estreitamente alinhadas aos objetivos de negócios, garantindo que os esforços de monitoramento estejam sempre a serviço de resultados comerciais tangíveis.

Antipadrões comuns:

- KPIs indefinidos: trabalhar sem KPIs claros pode levar ao monitoramento excessivo ou insuficiente, perdendo sinais vitais.
- KPIs estáticos: não revisar ou refinar os KPIs à medida que a workload ou os objetivos de negócios evoluem.
- Desalinhamento: foco em métricas técnicas que não se correlacionam diretamente com os resultados comerciais ou são mais difíceis de correlacionar com problemas do mundo real.

Benefícios de estabelecer esta prática recomendada:

- Facilidade de identificação de problemas: os KPIs de negócios geralmente mostram os problemas com mais clareza do que as métricas técnicas. Uma queda em um KPI comercial pode identificar um problema com mais eficiência do que analisar várias métricas técnicas.
- Alinhamento comercial: garante que as atividades de monitoramento apoiem diretamente os objetivos de negócios.
- Eficiência: priorize os recursos de monitoramento e a atenção nas métricas que importam.
- Proatividade: reconheça e resolva os problemas antes que eles tenham implicações comerciais mais amplas.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

Para definir com eficácia os KPIs da workload:

1. Comece com os resultados comerciais: Antes de mergulhar nas métricas, entenda o resultado comercial desejado. É aumento de vendas, maior engajamento do usuário ou tempos de resposta mais rápidos?
2. Correlacione métricas técnicas com objetivos de negócios: Nem todas as métricas técnicas têm um impacto direto nos resultados comerciais. Identifique aquelas que têm, mas geralmente é mais fácil identificar um problema usando um KPI comercial.
3. Use o [Amazon CloudWatch](#): Empregue o CloudWatch para definir e monitorar métricas que representam seus KPIs.
4. Revise e atualize regularmente os KPIs: À medida que sua workload e seus negócios evoluem, mantenha seus KPIs relevantes.
5. Envolver as partes interessadas: Envolver as equipes técnicas e comerciais na definição e revisão dos KPIs.

Nível de esforço do plano de implementação: médio

Recursos

Práticas recomendadas relacionadas:

- [the section called “OPS04-BP02 Implementar a telemetria de aplicações”](#)
- [the section called “OPS04-BP03 Implementar a telemetria da experiência do usuário”](#)
- [the section called “OPS04-BP04 Implementar a telemetria de dependências”](#)
- [the section called “OPS04-BP05 Implementar rastreamento distribuído”](#)

Documentos relacionados:

- [AWS Observability Best Practices \(Práticas recomendadas de observabilidade da AWS \)](#)
- [Guia do usuário do CloudWatch](#)
- [AWS Observability Skill Builder Course \(Curso de desenvolvimento de habilidades de observabilidade da AWS\)](#)

Vídeos relacionados:

- [Developing an observability strategy \(Desenvolvimento de uma estratégia de observabilidade\)](#)

Exemplos relacionados:

- [Um workshop de observabilidade](#)

OPS04-BP02 Implementar a telemetria de aplicações

A telemetria de aplicações serve como base para a observabilidade da workload. É fundamental emitir uma telemetria que ofereça informações práticas sobre o estado de sua aplicação e a obtenção de resultados técnicos e comerciais. Da solução de problemas à medição do impacto de um novo recurso ou à garantia do alinhamento com os indicadores-chave de performance (KPIs) de negócios, a telemetria de aplicações informa a maneira como você cria, opera e desenvolve sua workload.

Métricas, logs e rastreamentos formam os três pilares principais da observabilidade. Eles servem como ferramentas de diagnóstico que descrevem o estado de sua aplicação. Com o tempo, eles auxiliam na criação de linhas de base e na identificação de anomalias. No entanto, para garantir o alinhamento entre as atividades de monitoramento e os objetivos de negócios, é fundamental definir e monitorar os KPIs. Os KPIs de negócios geralmente facilitam a identificação de problemas em comparação com métricas técnicas isoladas.

Outros tipos de telemetria, como monitoramento de usuários reais (RUM) e transações sintéticas, complementam essas fontes de dados primárias. O RUM oferece informações sobre as interações do usuário em tempo real, enquanto as transações sintéticas simulam possíveis comportamentos do usuário, ajudando a detectar gargalos antes que usuários reais os encontrem.

Resultado desejado: Obtenha insights acionáveis sobre o desempenho de sua workload. Esses insights permitem que você tome decisões proativas sobre otimização de desempenho, obtenha maior estabilidade da workload, simplifique os processos de CI/CD e utilize recursos de forma eficaz.

Antipadrões comuns:

- **Observabilidade incompleta:** negligência da incorporação da observabilidade em todas as camadas da workload, resultando em pontos cegos que podem obscurecer insights vitais sobre desempenho e comportamento do sistema.

- Visualização fragmentada dos dados: quando os dados estão espalhados por várias ferramentas e sistemas, torna-se difícil manter uma visão holística da integridade e do desempenho de sua workload.
- Problemas relatados pelo usuário: um sinal de que falta a detecção proativa de problemas por meio da telemetria e do monitoramento de KPI de negócios.

Benefícios de estabelecer esta prática recomendada:

- Tomada de decisão informada: com insights de telemetria e KPIs de negócios, você pode tomar decisões baseadas em dados.
- Eficiência operacional aprimorada: a utilização de recursos baseada em dados leva à economia de custos.
- Estabilidade aprimorada da workload: detecção e resolução de problemas mais rápidas, levando a um melhor tempo de atividade.
- Processos simplificados de CI/CD: os insights dos dados de telemetria facilitam o refinamento dos processos e a entrega confiável do código.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

Para implementar a telemetria de aplicações para sua workload, use serviços da AWS, como o [Amazon CloudWatch](#) e o [AWS X-Ray](#). O Amazon CloudWatch fornece um conjunto abrangente de ferramentas de monitoramento, permitindo que você observe seus recursos e aplicações em ambientes da AWS e on-premises. Ele coleta, rastreia e analisa métricas, consolida e monitora dados de log e responde às mudanças em seus recursos, aprimorando sua compreensão de como a workload opera. Em conjunto, o AWS X-Ray permite rastrear, analisar e depurar suas aplicações, oferecendo uma compreensão profunda do comportamento da sua workload. Com recursos como mapas de serviços, distribuições de latência e cronogramas de rastreamento, o X-Ray fornece informações sobre o desempenho da workload e os gargalos que a afetam.

Etapas da implementação

1. Identifique quais dados coletar: Garanta as métricas, os logs e os rastreamentos essenciais que ofereceriam informações substanciais sobre a integridade, o desempenho e o comportamento de sua workload.

2. Implemente o agente do [CloudWatch](#) : O agente do CloudWatch é fundamental na aquisição de métricas do sistema e da aplicação e de logs de sua workload e de sua infraestrutura subjacente. O agente do CloudWatch também pode ser usado para coletar OpenTelemetry ou rastreamentos do X-Ray e enviá-los para o X-Ray.
3. Defina e monitore os KPIs de negócios: Estabeleça [métricas personalizadas](#) que se alinham com os seus [resultados empresariais](#).
4. Instrumente sua aplicação com o AWS X-Ray: além de implantar o agente do CloudWatch, é fundamental [instrumentar sua aplicação](#) para emitir dados de rastreamento. Esse processo pode fornecer mais informações sobre o comportamento e o desempenho da sua workload.
5. Padronize a coleta de dados em sua aplicação: Padronize as práticas de coleta de dados em toda a sua aplicação. A uniformidade ajuda a correlacionar e analisar dados, fornecendo uma visão abrangente do comportamento de sua aplicação.
6. Analise e aja com base nos dados: Depois que a coleta e a normalização de dados estiverem em vigor, use o [Amazon CloudWatch](#) para análise de métricas e logs e o [AWS X-Ray](#) para análise de rastreamentos. Essa análise pode gerar informações cruciais sobre a integridade, o desempenho e o comportamento de sua workload, orientando o processo de tomada de decisão.

Nível de esforço do plano de implementação: Alto

Recursos

Práticas recomendadas relacionadas:

- [OPS04-BP01 Identificar os indicadores-chave de performance](#)
- [OPS04-BP03 Implementar a telemetria da experiência do usuário](#)
- [OPS04-BP04 Implementar a telemetria de dependências](#)
- [OPS04-BP05 Implementar rastreamento distribuído](#)

Documentos relacionados:

- [AWS Observability Best Practices \(Práticas recomendadas de observabilidade da AWS \)](#)
- [Guia do usuário do CloudWatch](#)
- [Guia do desenvolvedor do AWS X-Ray](#)
- [Instrumentação de sistemas distribuídos para visibilidade operacional](#)

- [AWS Observability Skill Builder Course \(Curso de desenvolvimento de habilidades de observabilidade da AWS\)](#)
- [Quais são as novidades do Amazon CloudWatch?](#)
- [Quais são as novidades do AWS X-Ray?](#)

Vídeos relacionados:

- [AWS re:Invent 2022 - Observability best practices at Amazon \(AWS re:Invent 2022: práticas recomendadas de observabilidade na Amazon\)](#)
- [AWS re:Invent 2022 - Developing an observability strategy \(AWS re:Invent 2022: desenvolvimento de uma estratégia de observabilidade\)](#)

Exemplos relacionados:

- [Um workshop de observabilidade](#)
- [Biblioteca de soluções da AWS: monitoramento de aplicações com Amazon CloudWatch](#)

OPS04-BP03 Implementar a telemetria da experiência do usuário

É essencial obter insights profundos sobre as experiências dos clientes e as interações com sua aplicação. O monitoramento de usuários reais (RUM) e as transações sintéticas servem como ferramentas poderosas para essa finalidade. O RUM fornece dados sobre interações reais do usuário, oferecendo uma perspectiva não filtrada da satisfação do usuário, enquanto as transações sintéticas simulam as interações do usuário, ajudando a detectar possíveis problemas antes mesmo que eles afetem os usuários reais.

Resultado desejado: Uma visão holística da experiência do cliente, detecção proativa de problemas e otimização das interações do usuário para oferecer experiências digitais perfeitas.

Antipadrões comuns:

- Aplicações sem monitoramento de usuários reais (RUM):
 - Detecção atrasada de problemas: sem o RUM, talvez você não fique ciente dos gargalos ou problemas de desempenho até que os usuários reclamem. Essa abordagem reativa pode levar à insatisfação do cliente.

- Falta de insights sobre a experiência do usuário: não usar o RUM significa perder dados cruciais que mostram como usuários reais interagem com sua aplicação, limitando sua capacidade de otimizar a experiência do usuário.
- Aplicações sem transações sintéticas:
 - Casos extremos perdidos: transações sintéticas ajudam você a testar caminhos e funções que podem não ser usados com frequência por usuários comuns, mas são essenciais para determinadas funções de negócios. Sem eles, esses caminhos podem ter problemas de funcionamento e passar despercebidos.
 - Verificação de problemas quando a aplicação não está sendo usada: testes sintéticos regulares podem simular momentos em que usuários reais não estão interagindo ativamente com sua aplicação, garantindo que o sistema sempre funcione corretamente.

Benefícios de estabelecer esta prática recomendada:

- Detecção proativa de problemas: identifique e resolva possíveis problemas antes que eles afetem usuários reais.
- Experiência otimizada do usuário: o feedback contínuo do RUM ajuda a refinar e aprimorar a experiência geral do usuário.
- Informações sobre o desempenho do dispositivo e do navegador: entenda o desempenho da sua aplicação em vários dispositivos e navegadores, permitindo uma maior otimização.
- Fluxos de trabalho de negócios validados: transações sintéticas regulares garantem que as principais funcionalidades e os caminhos críticos permaneçam operacionais e eficientes.
- Desempenho aprimorado da aplicação: utilize as informações coletadas de dados reais do usuário para melhorar a capacidade de resposta e a confiabilidade da aplicação.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

Para aproveitar o RUM e as transações sintéticas para a telemetria da atividade do usuário, a AWS oferece serviços como [Amazon CloudWatch RUM](#) e [Amazon CloudWatch Synthetics](#). Métricas, logs e rastreamentos, juntamente com dados de atividades do usuário, fornecem uma visão abrangente do estado operacional da aplicação e da experiência do usuário.

Etapas da implementação

1. Implemente o Amazon CloudWatch RUM: integre sua aplicação ao CloudWatch RUM para coletar, analisar e apresentar dados reais do usuário.
 - a. Use a [biblioteca em JavaScript do CloudWatch](#) para integrar o RUM à sua aplicação.
 - b. Configure painéis para visualizar e monitorar dados reais do usuário.
2. Configuração do CloudWatch Synthetics: crie canários ou rotinas com script que simulem as interações do usuário com sua aplicação.
 - a. Defina fluxos de trabalho e caminhos de aplicação críticos.
 - b. Projete canários usando [scripts do CloudWatch](#) para simular as interações do usuário nesses caminhos.
 - c. Programe e monitore os canários para serem executados em intervalos específicos, garantindo verificações de desempenho consistentes.
3. Analise e aja com base nos dados: Utilize dados de RUM e transações sintéticas para obter insights e tomar medidas corretivas quando anomalias forem detectadas. Use painéis do CloudWatch e alarmes para se manter informado.

Nível de esforço do plano de implementação: médio

Recursos

Práticas recomendadas relacionadas:

- [OPS04-BP01 Identificar os indicadores-chave de performance](#)
- [OPS04-BP02 Implementar a telemetria de aplicações](#)
- [OPS04-BP04 Implementar a telemetria de dependências](#)
- [OPS04-BP05 Implementar rastreamento distribuído](#)

Documentos relacionados:

- [Guia do Amazon CloudWatch RUM](#)
- [Guia do Amazon CloudWatch Synthetics](#)

Vídeos relacionados:

- [Optimize applications through end user insights with Amazon CloudWatch RUM \(Otimização de aplicações por meio de insights sobre o usuário final com o Amazon CloudWatch RUM\)](#)
- [AWS on Air ft. Real-User Monitoring for Amazon CloudWatch \(Monitoramento de usuários reais do Amazon CloudWatch\)](#)

Exemplos relacionados:

- [Um workshop de observabilidade](#)
- [Repositório Git do Amazon CloudWatch RUM Web Client](#)
- [Uso do Amazon CloudWatch Synthetics para medir o tempo de carregamento da página](#)

OPS04-BP04 Implementar a telemetria de dependências

A telemetria de dependências é essencial para monitorar a integridade e a performance dos serviços e componentes externos dos quais a workload depende. Ela fornece informações valiosas sobre acessibilidade, tempos limite e outros eventos críticos relacionados a dependências, como DNS, bancos de dados ou APIs de terceiros. Ao instrumentar sua aplicação para emitir métricas, logs e rastreamentos sobre essas dependências, você obtém uma compreensão mais clara dos possíveis gargalos, problemas de performance ou falhas que podem afetar a workload.

Resultado desejado: As dependências das quais a workload depende estão funcionando conforme o esperado, permitindo que você resolva problemas de forma proativa e garanta a performance ideal da workload.

Antipadrões comuns:

- Negligenciar as dependências externas: focar apenas nas métricas internas da aplicação e negligenciar as métricas relacionadas às dependências externas.
- Falta de monitoramento proativo: aguardar o surgimento de problemas em vez de monitorar continuamente a integridade e a performance da dependência.
- Monitoramento em silos: usar várias ferramentas de monitoramento diferentes, o que pode resultar em visualizações fragmentadas e inconsistentes da integridade da dependência.

Benefícios de estabelecer esta prática recomendada:

- Maior confiabilidade da workload: garantindo que as dependências externas estejam consistentemente disponíveis e tenham uma performance ideal.

- Detecção e resolução mais rápidas de problemas: identificação e resolução proativa de problemas com dependências antes que elas afetem a workload.
- Visão abrangente: obtendo uma visão holística dos componentes internos e externos que influenciam a integridade da workload.
- Escalabilidade aprimorada da workload: entendendo os limites de escalabilidade e as características de performance das dependências externas.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

Implemente a telemetria de dependências começando com a identificação dos serviços, da infraestrutura e dos processos dos quais a workload depende. Quantifique quais são as boas condições quando essas dependências estão funcionando conforme o esperado e determine quais dados são necessários para medi-las. Com essas informações, você pode criar painéis e alertas que fornecem insights para suas equipes de operações sobre o estado dessas dependências. Use ferramentas da AWS para descobrir e quantificar os impactos quando as dependências não puderem desempenhar conforme necessário. Revise continuamente sua estratégia para considerar as mudanças nas prioridades, metas e insights obtidos.

Etapas da implementação

Para implementar a telemetria de dependências de forma eficaz:

1. Identifique dependências externas: colabore com as partes interessadas para identificar as dependências externas das quais a workload depende. As dependências externas podem abranger serviços como bancos de dados externos, APIs de terceiros, rotas de conectividade de rede para outros ambientes e serviços de DNS. O primeiro passo para uma telemetria de dependências eficaz é entender de forma abrangente quais são essas dependências.
2. Desenvolva uma estratégia de monitoramento: depois de ter uma visão clara de suas dependências externas, elabore uma estratégia de monitoramento personalizada para elas. Isso envolve entender a importância de cada dependência, seu comportamento esperado e quaisquer contratos ou metas de nível de serviço associados (SLA ou SLTs). Configure alertas proativos para receber notificações sobre mudanças de status ou desvios de performance.
3. Utilize o [Amazon CloudWatch Internet Monitor](#): ele oferece informações sobre a internet global, ajudando a entender interrupções que podem afetar suas dependências externas.

4. Mantenha-se informado com o [AWS Health Dashboard](#): ele fornece alertas e orientações de correção quando a AWS está enfrentando eventos que podem impactar seus serviços.
5. Instrumente sua aplicação com o [AWS X-Ray](#): o AWS X-Ray fornece informações sobre a performance das aplicações e de suas respectivas dependências subjacentes. Ao rastrear as solicitações do início ao fim, você pode identificar gargalos ou falhas nos serviços ou componentes externos dos quais sua aplicação depende.
6. Use o [Amazon DevOps Guru](#): esse serviço orientado por machine learning identifica problemas operacionais, prevê quando problemas críticos podem ocorrer e recomenda ações específicas a serem tomadas. Ele é inestimável para obter informações sobre dependências e determinar que elas não são a fonte dos problemas operacionais.
7. Monitore regularmente: monitore continuamente métricas e logs relacionados a dependências externas. Configure alertas para comportamento inesperado ou diminuição de performance.
8. Valide após as alterações: sempre que houver uma atualização ou alteração em qualquer uma das dependências externas, valide sua performance e verifique o alinhamento com os requisitos da sua aplicação.

Nível de esforço do plano de implementação: médio

Recursos

Práticas recomendadas relacionadas:

- [OPS04-BP01 Identificar os indicadores-chave de performance](#)
- [OPS04-BP02 Implementar a telemetria de aplicações](#)
- [OPS04-BP03 Implementar a telemetria da experiência do usuário](#)
- [OPS04-BP05 Implementar rastreamento distribuído](#)

Documentos relacionados:

- [O que é o AWS Health?](#)
- [Uso do Amazon CloudWatch Internet Monitor](#)
- [Guia do desenvolvedor do AWS X-Ray](#)
- [Guia do usuário do Amazon DevOps Guru](#)

Vídeos relacionados:

- [Visibility into how internet issues impact app performance](#)
- [Introduction to Amazon DevOps Guru \(Introdução ao Amazon DevOps Guru\)](#)

Exemplos relacionados:

- [Gaining operational insights with AIOps using Amazon DevOps Guru](#)
- [AWS Health Aware](#)

OPS04-BP05 Implementar rastreamento distribuído

O rastreamento distribuído oferece uma maneira de monitorar e visualizar solicitações à medida que elas percorrem vários componentes de um sistema distribuído. Ao capturar dados de rastreamento de várias fontes e analisá-los em uma visão unificada, as equipes podem entender melhor como as solicitações fluem, onde existem gargalos e onde os esforços de otimização devem se concentrar.

Resultado desejado: Obtenha uma visão holística das solicitações que fluem pelo seu sistema distribuído, permitindo depuração precisa, desempenho otimizado e experiências de usuário aprimoradas.

Antipadrões comuns:

- Instrumentação inconsistente: nem todos os serviços em um sistema distribuído são instrumentados para rastreamento.
- Ignorar a latência: foco apenas nos erros e sem considerar a latência ou as degradações graduais do desempenho.

Benefícios de estabelecer esta prática recomendada:

- Visão geral abrangente do sistema: visualização de todo o caminho das solicitações, da entrada à saída.
- Depuração aprimorada: identificação rápida de onde ocorrem falhas ou problemas de desempenho.
- Experiência de usuário aprimorada: monitoramento e otimização com base nos dados reais do usuário, garantindo que o sistema atenda às demandas do mundo real.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

Comece identificando todos os elementos da workload que exigem instrumentação. Depois que todos os componentes forem contabilizados, utilize ferramentas como o AWS X-Ray e o OpenTelemetry para coletar dados de rastreamento para análise com ferramentas como o X-Ray e o Amazon CloudWatch ServiceLens Map. Faça avaliações regulares com desenvolvedores e complemente essas discussões com ferramentas como Amazon DevOps Guru X-Ray Analytics e X-Ray Insights para ajudar a fazer descobertas mais profundas. Estabeleça alertas a partir de dados de rastreamento para notificar quando os resultados, conforme definido no plano de monitoramento da workload, estiverem em risco.

Etapas da implementação

Para implementar o rastreamento distribuído de forma eficaz:

1. Use o [AWS X-Ray](#): integre o X-Ray à sua aplicação para obter informações sobre seu comportamento, entender seu desempenho e identificar gargalos. Utilize o X-Ray Insights para análise automática de rastreamento.
2. Instrumente seus serviços: verifique se cada serviço, de uma função do [AWS Lambda](#) a uma [instância do EC2](#), envia dados de rastreamento. Quanto mais serviços você instrumentar, mais clara será a visão completa.
3. incorpore o [monitoramento de usuários reais do CloudWatch](#) e o [monitoramento sintético](#): integre o monitoramento de usuários reais (RUM) e o monitoramento sintético com o X-Ray. Isso permite capturar experiências reais do usuário e simular as interações do usuário para identificar possíveis problemas.
4. Use o [agente do CloudWatch](#): o agente pode enviar rastreamentos a partir do X-Ray ou do OpenTelemetry, aumentando a profundidade dos insights obtidos.
5. Use o [Amazon DevOps Guru](#): o DevOps Guru usa dados do X-Ray, CloudWatch, AWS Config e AWS CloudTrail para fornecer recomendações práticas.
6. Analise os rastreamentos: analise regularmente os dados de rastreamento para discernir padrões, anomalias ou gargalos que possam afetar o desempenho de sua aplicação.
7. Configure alertas: configure os alarmes no [CloudWatch](#) para padrões incomuns ou latências estendidas, permitindo o tratamento proativo de problemas.
8. Melhoria contínua: revise sua estratégia de rastreamento à medida que os serviços são adicionados ou modificados para capturar todos os pontos de dados relevantes.

Nível de esforço do plano de implementação: médio

Recursos

Práticas recomendadas relacionadas:

- [OPS04-BP01 Identificar os indicadores-chave de performance](#)
- [OPS04-BP02 Implementar a telemetria de aplicações](#)
- [OPS04-BP03 Implementar a telemetria da experiência do usuário](#)
- [OPS04-BP04 Implementar a telemetria de dependências](#)

Documentos relacionados:

- [Guia do desenvolvedor do AWS X-Ray](#)
- [Guia do usuário do agente do Amazon CloudWatch](#)
- [Guia do usuário do Amazon DevOps Guru](#)

Vídeos relacionados:

- [Use AWS X-Ray Insights \(Use o AWS X-Ray Insights\)](#)
- [AWS on Air ft. Observability: Amazon CloudWatch and AWS X-Ray \(Observabilidade: Amazon CloudWatch e AWS X-Ray\)](#)

Exemplos relacionados:

- [Instrumentação da aplicação com AWS X-Ray](#)

Design das operações

Adote abordagens que melhoram o fluxo de alterações na produção e ajudam na refatoração, em comentários rápidos sobre a qualidade e na correção de erros. Isso acelera as alterações benéficas que entram na produção, limita os problemas implantados e oferece rápida identificação e correção dos problemas introduzidos pelas atividades de implantação.

Na AWS, é possível visualizar a workload completa (aplicações, infraestrutura, política, governança e operações) como código. Tudo pode ser definido e atualizado usando o código. Isso significa que

you can apply the same engineering discipline used for the application code to all elements of your stack.

Práticas recomendadas

- [OPS05-BP01 Usar o controle de versão](#)
- [OPS05-BP02 Testar e valide as alterações](#)
- [OPS05-BP03 Usar sistemas de gerenciamento de configuração](#)
- [OPS05-BP04 Usar sistemas de gerenciamento de compilação e de implantação](#)
- [OPS05-BP05 Executar o gerenciamento de patches](#)
- [OPS05-BP06 Compartilhar os padrões de design](#)
- [OPS05-BP07 Implementar práticas para aprimorar a qualidade do código](#)
- [OPS05-BP08 Usar vários ambientes](#)
- [OPS05-BP09 Fazer alterações frequentes, pequenas e reversíveis](#)
- [OPS05-BP10 Automatizar totalmente a integração e a implantação](#)

OPS05-BP01 Usar o controle de versão

Use version control to enable tracking of changes and releases.

Many AWS services offer version control resources. Use a revision or source control system such as [AWS CodeCommit](#) to manage code and other artifacts, or [AWS CloudFormation](#) models with version control of your infrastructure.

Resultado desejado: Your teams collaborate on code. When merged, the code is consistent and no change is lost. Errors are easily reverted through the correct versioning.

Antipadrões comuns:

- You are developing and storing your code on your workstation. You had a storage failure on your workstation and your code was lost.
- After replacing existing code with changes, you restart the application and it becomes unoperable. It is not possible to revert the change.
- You have a file lock on a report file that another person needs to edit. She contacts you requesting that you interrupt your work so that she can complete her tasks.

- Sua equipe de pesquisa tem trabalhado em uma análise detalhada que moldará seu trabalho futuro. Alguém salvou acidentalmente a lista de compras sobre relatório final. Não é possível reverter a alteração e você terá que recriar o relatório.

Benefícios de estabelecer esta prática recomendada: Ao usar recursos de versionamento, você pode reverter facilmente para bons estados conhecidos, versões anteriores e limitar o risco de perda de ativos.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

Mantenha ativos em repositórios controlados por versão. Fazer isso oferece suporte para o rastreamento de alterações, a implantação de novas versões, a detecção de alterações nas versões existentes e a reversão para versões anteriores (por exemplo, a reversão para um estado bom e conhecido no caso de uma falha). Integre os recursos de controle de versão dos sistemas de gerenciamento de configurações aos seus procedimentos.

Recursos

Práticas recomendadas relacionadas:

- [OPS05-BP04 Usar sistemas de gerenciamento de compilação e de implantação](#)

Documentos relacionados:

- [O que é o AWS CodeCommit?](#)

Vídeos relacionados:

- [Introduction to AWS CodeCommit \(Introdução ao AWS CodeCommit\)](#)

OPS05-BP02 Testar e valide as alterações

Cada alteração implantada deve ser testada para evitar erros na produção. A prática recomendada concentra-se em testar alterações do controle de versão na build de artefato. Além das alterações do código da aplicação, o teste deve incluir infraestrutura, configuração, controles de segurança e procedimentos de operações. O teste assume muitas formas, desde testes de unidade à análise dos

componentes do software (SCA). Mova os testes mais para a esquerda na integração do software e o processo de entrega resultará em maior certeza da qualidade do artefato.

Sua organização deve desenvolver padrões de teste para todos os artefatos de software. Os testes automatizados reduzem o trabalho e evitam erros de testes manuais. Os testes manuais podem ser necessários em alguns casos. Os desenvolvedores precisam ter acesso aos resultados dos testes automatizados para criar loops de feedback que melhorem a qualidade do software.

Resultado desejado: As alterações do software são testadas antes de serem entregues. Os desenvolvedores têm acesso aos resultados e validações dos testes. Sua organização tem um padrão de testes que se aplica a todas as alterações do software.

Antipadrões comuns:

- Você implanta uma nova alteração do software sem nenhum teste. Ele não é executado na produção, o que ocasiona uma interrupção.
- Novos grupos de segurança são implantados com o AWS CloudFormation sem serem testados em um ambiente de pré-produção. Os grupos de segurança tornam sua aplicação inacessível para seus clientes.
- Um método é modificado, mas não há testes de unidade. O software falha quando é implantado em produção.

Benefícios de estabelecer esta prática recomendada: A taxa de falha de alteração de implantações de software é reduzida. A qualidade do software é aprimorada. Os desenvolvedores aumentaram a conscientização sobre a viabilidade do código deles. As políticas de segurança podem ser distribuídas com confiança para apoiar a conformidade da organização. Alterações da infraestrutura, como atualizações da política de ajuste de escala automático, são testadas com antecedência para atender às necessidades de tráfego.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

Testes são realizados em todas as alterações, desde o código da aplicação à infraestrutura, como parte de sua prática de integração contínua. Os resultados dos testes são publicados para que os desenvolvedores tenham feedback rápido. Sua organização tem um padrão de testes de que todas as alterações devem ser aprovadas.

Exemplo de clientes

Como parte do pipeline de integração contínua, a AnyCompany Retail realiza alguns tipos de teste em todos os artefatos de software. Eles praticam desenvolvimento orientado a testes para que todo o software tenha testes de unidade. Depois que o artefato é criado, eles executam testes completos. Depois que a primeira etapa de testes é concluída, eles executam uma verificação de segurança da aplicação estática, que procura vulnerabilidades conhecidas. Os desenvolvedores recebem mensagens à medida que cada gate de testes é aprovado. Depois que todos os testes são concluídos, o artefato de software é armazenado em um repositório de artefatos.

Etapas da implementação

1. Trabalhe com partes interessadas em sua organização para desenvolver um padrão de testes para artefatos de software. Em quais testes padrão todos os artefatos devem ser aprovados? Há requisitos de conformidade ou governança que devem ser incluídos na cobertura de testes? Você precisa realizar testes de qualidade de código? Quando os testes são concluídos, quem precisa saber?
 - a. A [arquitetura de referência de pipeline de implantação da AWS](#) contém uma lista confiável de tipos de testes que podem ser conduzidos em artefatos de software como parte de um pipeline de integração.
2. Instrumente sua aplicação com os testes necessários com base em seu padrão de testes de software. Cada conjunto de testes deve ser concluído em menos de dez minutos. Os testes devem ser executados como parte de um pipeline de integração.
 - a. [O Amazon CodeGuru Reviewer](#) pode testar seu código de aplicação quanto a defeitos.
 - b. Você pode usar o [AWS CodeBuild](#) para realizar testes em artefatos de software.
 - c. [O AWS CodePipeline](#) pode orquestrar seus testes de software em um pipeline.

Recursos

Práticas recomendadas relacionadas:

- [OPS05-BP01 Usar o controle de versão](#)
- [OPS05-BP06 Compartilhar os padrões de design](#)
- [OPS05-BP10 Automatizar totalmente a integração e a implantação](#)

Documentos relacionados:

- [Adopt a test-driven development approach \(Adotar uma abordagem de desenvolvimento orientada a testes\)](#)
- [Automated AWS CloudFormation Testing Pipeline with TaskCat and CodePipeline \(Pipeline de teste do AWS CloudFormation automatizado com TaskCat e CodePipeline\)](#)
- [Building end-to-end AWS DevSecOps CI/CD pipeline with open source SCA, SAST, and DAST tools \(Criar um pipeline de CI/CD completo do AWS DevSecOps e ferramentas DAST\)](#)
- [Getting started with testing serverless applications \(Conceitos básicos de testes de aplicações com tecnologia sem servidor\)](#)
- [My CI/CD pipeline is my release captain \(Meu pipeline de CI/CD é meu capitão de lançamentos\)](#)
- [Whitepaper: Practicing Continuous Integration and Continuous Delivery on AWS \(Praticar a integração e entrega contínuas na AWS\)](#)

Vídeos relacionados:

- [AWS re:Invent 2020: Testable infrastructure: Integration testing on AWS \(AWS re:Invent 2020: infraestrutura testável: teste de integração na AWS\)](#)
- [AWS Summit ANZ 2021 - Driving a test-first strategy with CDK and test driven development \(AWS Summit ANZ 2021: conduzir uma estratégia de primeiro teste com o CDK e desenvolvimento orientado a testes\)](#)
- [Testing Your Infrastructure as Code with AWS CDK \(Testar sua infraestrutura como código com o AWS CDK\)](#)

Recursos relacionados:

- [AWS Deployment Pipeline Reference Architecture - Application \(Arquitetura de referência de pipeline de implantação da AWS: aplicação\)](#)
- [AWS Kubernetes DevSecOps Pipeline \(Pipeline do AWS Kubernetes DevSecOps\)](#)
- [Workshop sobre política como código: desenvolvimento orientado a testes](#)
- [Run unit tests for a Node.js application from GitHub by using AWS CodeBuild \(Executar testes de unidade para uma aplicação Node.js do GitHub usando o AWS CodeBuild\)](#)
- [Use Serverspec for test-driven development of infrastructure code \(Usar o Serverspec para desenvolvimento orientado a testes do código de infraestrutura\)](#)

Serviços relacionados:

- [Amazon CodeGuru Reviewer](#)
- [AWS CodeBuild](#)
- [AWS CodePipeline](#)

OPS05-BP03 Usar sistemas de gerenciamento de configuração

Use os sistemas de gerenciamento de configuração para fazer e rastrear alterações nas configurações. Esses sistemas reduzem os erros causados pelos processos manuais e o nível de esforço para implantar as alterações.

O gerenciamento da configuração estática define valores ao inicializar um recurso que deve permanecer consistente durante todo o tempo de vida do recurso. Alguns exemplos incluem a definição da configuração do servidor web ou de aplicação em uma instância, ou a definição da configuração de um serviço da AWS no [AWS Management Console](#) ou por meio da [AWS CLI](#).

O gerenciamento da configuração dinâmica define valores na inicialização que podem ou devem ser alterados durante o tempo de vida de um recurso. Por exemplo, é possível definir a alternância de um recurso para ativar uma funcionalidade no código por meio de uma alteração na configuração, ou alterar o nível de detalhes do log durante um incidente para capturar mais dados e desfazer a alteração depois do incidente, eliminando os logs agora desnecessários e a despesa associada.

Na AWS, você pode usar o [AWS Config](#) para monitorar continuamente as configurações de seus recursos da AWS [entre contas e Regiões](#). Isso ajuda a rastrear o histórico da configuração, compreender como a alteração de uma configuração afeta outros recursos e auditá-la em relação a configurações esperadas ou desejadas, usando o [Regras do AWS Config](#) e [pacotes de conformidade do AWS Config](#).

Se tiver configurações dinâmicas em suas aplicações executadas em instâncias do Amazon EC2, AWS Lambda, contêineres, aplicativos móveis ou dispositivos de IoT, você pode usar o [AWS AppConfig](#) para configurá-las, validá-las, implantá-las e monitorá-las em seus ambientes.

Na AWS, é possível criar pipelines de integração contínua/implantação contínua (CI/CD) usando serviços como as [Ferramentas de desenvolvedor da AWS](#) (por exemplo: o [AWS CodeCommit](#), o [AWS CodeBuild](#), o [AWS CodePipeline](#), o [AWS CodeDeploy](#) e o [AWS CodeStar](#)).

Resultado desejado: Você configura, valida e implanta como parte de seu pipeline de integração contínua e entrega contínua (CI/CD). Você monitora para validar se as configurações estão corretas. Isso minimiza qualquer impacto para usuários finais e clientes.

Antipadrões comuns:

- Você atualiza manualmente a configuração do servidor web em toda a frota e vários servidores não respondem devido a erros de atualização.
- Você atualiza manualmente a frota do servidor de aplicativos ao longo de muitas horas. A inconsistência na configuração durante a alteração causa comportamentos inesperados.
- Alguém atualizou seus grupos de segurança e seus servidores web não estão mais acessíveis. Sem saber o que foi alterado, você gasta muito tempo investigando o problema, ampliando o tempo de recuperação.
- Você coloca uma configuração de pré-produção em produção por meio de CI/CD sem validação. Você expõe usuários e clientes a dados e serviços incorretos.

Benefícios de estabelecer esta prática recomendada: A adoção de sistemas de gerenciamento de configurações reduz o nível de esforço para fazer e rastrear alterações, bem como a frequência de erros causados por procedimentos manuais. Os sistemas de gerenciamento de configuração fornecem garantias com relação aos requisitos regulatórios, de conformidade e de governança.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Os sistemas de gerenciamento de configuração são usados para rastrear e implementar alterações nas configurações de aplicações e ambientes. Os sistemas de gerenciamento de configuração também são usados para reduzir erros causados por processos manuais, tornar as alterações de configuração repetíveis e auditáveis e reduzir o nível de esforço.

Etapas da implementação

1. Identifique os proprietários da configuração.
 - a. Informe os proprietários das configurações sobre quaisquer necessidades regulatórias, de conformidade ou de controle.
2. Identifique os itens de configuração e os resultados.
 - a. Os itens de configuração são todas as configurações de aplicações e ambientes afetadas por uma implantação em seu pipeline de CI/CD.
 - b. Os resultados incluem critérios de sucesso, validação e o que monitorar.
3. Selecione ferramentas para gerenciamento de configuração com base nos requisitos de seus negócios e no pipeline de entrega.

4. Considere implantações ponderadas, como implantações canário, para alterações significativas na configuração, a fim de minimizar o impacto de configurações incorretas.
5. Integre seu gerenciamento de configuração ao seu pipeline de CI/CD.
6. Valide todas as alterações enviadas.

Recursos

Práticas recomendadas relacionadas:

- [OPS06-BP01 Preparar-se para alterações malsucedidas](#)
- [OPS06-BP02 Testar as implantações](#)
- [OPS06-BP03 Utilizar estratégias de implantação seguras](#)
- [OPS06-BP04 Automatizar os testes e a reversão](#)

Documentos relacionados:

- [AWS Control Tower](#)
- [AWS Landing Zone Accelerator \(Acelerador de zona de pouso da AWS\)](#)
- [AWS Config](#)
- [O que é o AWS Config?](#)
- [AWS AppConfig](#)
- [O que é o AWS CloudFormation?](#)
- [Ferramentas de desenvolvedor da AWS](#)

Vídeos relacionados:

- [AWS re:Invent 2022 - Proactive governance and compliance for AWS workloads \(AWS re:Invent 2022: governança e conformidade proativas para workloads da AWS\)](#)
- [AWS re:Invent 2020: Achieve compliance as code using AWS Config \(AWS re:Invent 2020: alcance a conformidade como código usando o AWS Config\)](#)
- [Manage and Deploy Application Configurations with AWS AppConfig \(Gerencie e implante configurações de aplicações com o AWS AppConfig\)](#)

OPS05-BP04 Usar sistemas de gerenciamento de compilação e de implantação

Use sistemas de gerenciamento de compilação e implantação. Esses sistemas reduzem os erros causados pelos processos manuais e o nível de esforço para implantar as alterações.

Na AWS, é possível criar pipelines de integração contínua/implantação contínua (CI/CD) usando serviços como [Ferramentas de desenvolvedor da AWS](#) (por exemplo, AWS CodeCommit, [AWS CodeBuild](#), o [AWS CodePipeline](#), o [AWS CodeDeploy](#) e o [AWS CodeStar](#)).

Resultado desejado: Seus sistemas de gerenciamento de compilação e implantação oferecem suporte ao sistema de integração contínua (CI/CD) de sua organização, que fornece recursos para automatizar implementações seguras com as configurações corretas.

Antipadrões comuns:

- Depois de compilar o código no sistema de desenvolvimento e copiar o executável nos sistemas de produção, há uma falha na inicialização. Os arquivos de log locais indicam que a falha ocorreu devido à ausência de dependências.
- Você cria a aplicação com êxito com os novos recursos em seu ambiente de desenvolvimento e fornece o código à garantia de qualidade (QA). Ele falha no QA porque não há ativos estáticos.
- Na sexta-feira, após muito esforço, você consegue criar a aplicação manualmente em seu ambiente de desenvolvimento, incluindo os recursos recém-codificados. Na segunda-feira, você não consegue repetir as etapas que permitiram criar a aplicação com êxito.
- Você executa os testes que criou para a nova versão. Então você passa a próxima semana configurando um ambiente de teste e executando todos os testes de integração existentes, seguidos pelos testes de performance. O novo código tem um impacto inaceitável na performance e deve ser desenvolvido e testado novamente.

Benefícios de estabelecer esta prática recomendada: Ao fornecer mecanismos para gerenciar atividades de criação e implantação, você reduz o nível de esforço para executar tarefas repetitivas, libera os membros da equipe para se concentrarem em tarefas criativas de alto valor e limita o surgimento de erros provenientes de procedimentos manuais.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Os sistemas de gerenciamento de compilação e implantação são usados para rastrear e implementar mudanças, reduzir erros causados por processos manuais e reduzir o nível de esforço necessário para implantações seguras. Automatize totalmente o pipeline de integração e implantação desde o check-in do código até a compilação, o teste, a implantação e a validação. Isso reduz o tempo de espera, diminui os custos, incentiva o aumento da frequência de mudanças, reduz o nível de esforço e aumenta a colaboração.

Etapas da implementação

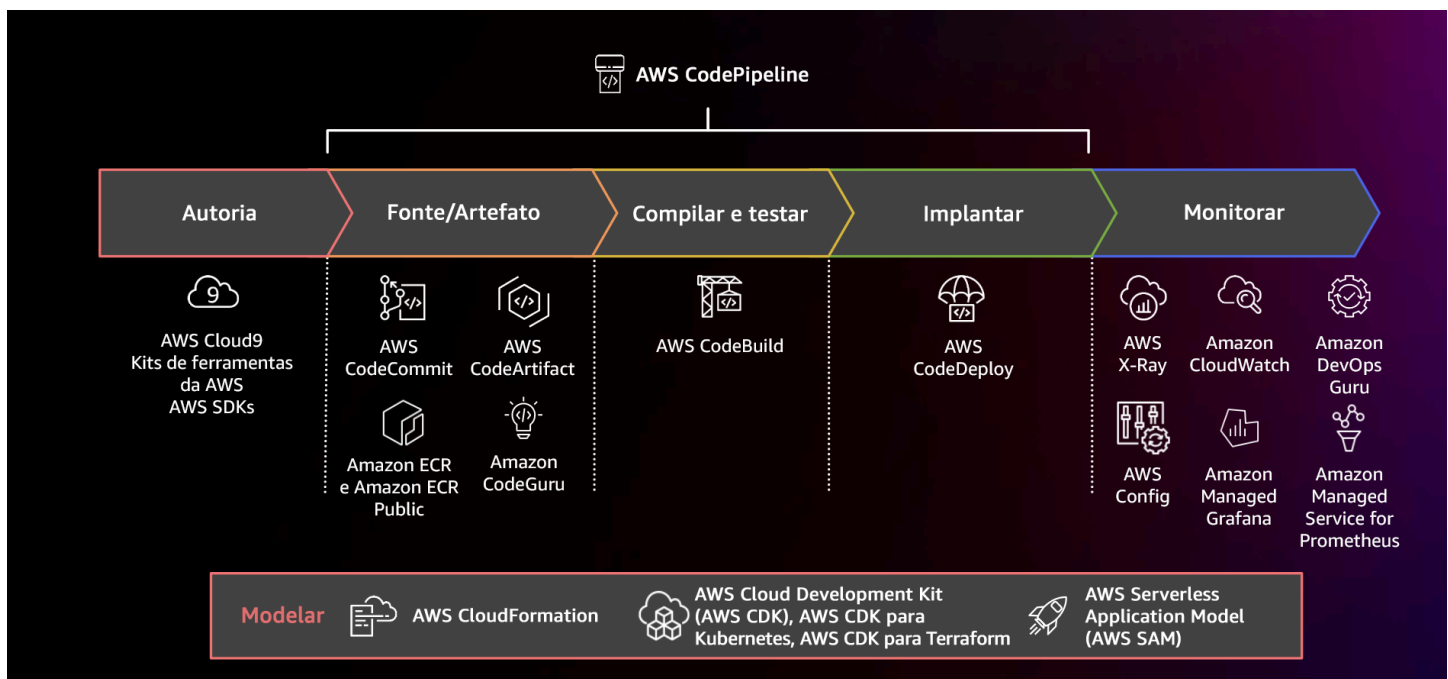


Diagrama mostrando um pipeline de CI/CD usando o AWS CodePipeline e serviços relacionados

1. Use o AWS CodeCommit para controlar versões, armazenar e gerenciar ativos (como documentos, código-fonte e arquivos binários).
2. Use o CodeBuild para compilar seu código-fonte, executar testes de unidade e produzir artefatos prontos para serem implantados.
3. Use CodeDeploy como serviço de implantação que automatiza as implantações de aplicações para [Amazon EC2](#) instâncias, instâncias on-premises, [funções do AWS Lambda sem servidor](#) ou [Amazon ECS](#).
4. Monitore suas implantações.

Recursos

Práticas recomendadas relacionadas:

- [OPS06-BP04 Automatizar os testes e a reversão](#)

Documentos relacionados:

- [Ferramentas de desenvolvedor da AWS](#)
- [O que é o AWS CodeCommit?](#)
- [O que é o AWS CodeBuild?](#)
- [AWS CodeBuild](#)
- [O que é o AWS CodeDeploy?](#)

Vídeos relacionados:

- [AWS re:Invent 2022 - AWS Well-Architected best practices for DevOps on AWS \(AWS re:Invent 2022: práticas recomendadas do AWS Well-Architected para DevOps na AWS\)](#)

OPS05-BP05 Executar o gerenciamento de patches

Execute o gerenciamento de patches para obter recursos, solucionar problemas e manter a conformidade com a governança. Automatize o gerenciamento de patches para reduzir erros causados por processos manuais, escalar e facilitar a realização de patches.

O gerenciamento de patches e vulnerabilidades faz parte de suas atividades de gerenciamento de benefícios e riscos. É preferível ter infraestruturas imutáveis e implantar cargas de trabalho em bons estados verificados e conhecidos. Quando isso não é viável, a aplicação de patches é a opção restante.

O [Amazon EC2 Image Builder](#) fornece pipelines para atualizar as imagens de máquina. Como parte do gerenciamento de patches, considere [Amazon Machine Images](#) (AMIs) usando um [pipeline de imagens AMI](#) ou imagens de contêiner com um [pipeline de imagens do Docker](#), enquanto o AWS Lambda fornece padrões para [tempos de execução personalizados e bibliotecas adicionais](#) para remover vulnerabilidades.

Você deve gerenciar atualizações em [Amazon Machine Images](#) para imagens do Linux ou Windows Server usando o [Amazon EC2 Image Builder](#). Você pode usar o [Amazon Elastic Container Registry](#)

([Amazon ECR](#)) com seu pipeline existente para gerenciar imagens do Amazon ECS e gerenciar imagens do Amazon EKS. O Lambda inclui [recursos de gerenciamento de versão](#).

A aplicação de patches não deve ser realizada em sistemas de produção sem antes testá-los em um ambiente seguro. Os patches só deverão ser aplicados se forem compatíveis com um resultado operacional ou comercial. Na AWS, você pode usar o [AWS Systems Manager Patch Manager](#) para automatizar o processo de aplicação de patches em sistemas gerenciados e programar a atividade usando o [Systems Manager Maintenance Windows](#).

Resultado desejado: suas imagens de AMI e contêiner foram corrigidas, atualizadas e estão prontas para o lançamento. Você pode acompanhar o status de todas as imagens implantadas e conhecer a conformidade do patch. É possível emitir relatórios do status atual e ter um processo para atender às suas necessidades de conformidade.

Antipadrões comuns:

- Você recebe uma ordem para aplicar todos os novos patches de segurança em até duas horas, resultando em várias interrupções devido à incompatibilidade da aplicação com os patches.
- Uma biblioteca sem patches resulta em consequências indesejadas, pois partes desconhecidas usam vulnerabilidades dentro dela para acessar a workload.
- Você aplica patches nos ambientes do desenvolvedor automaticamente, sem notificar os desenvolvedores. Você recebe várias reclamações dos desenvolvedores, dizendo que o ambiente deles não está funcionando conforme o esperado.
- Você não aplicou patches no software pronto para uso comercial em uma instância persistente. Quando você tiver um problema com o software e entrar em contato com o fornecedor, ele informará que a versão não é compatível e será necessário aplicar patches a um nível específico para receber assistência.
- Um patch lançado recentemente para o software de criptografia que você usou tem melhorias significativas de performance. Seu sistema sem patches tem problemas de performance que permanecem enquanto não for feita a aplicação de patches.
- Você é notificado sobre uma vulnerabilidade de dia zero que exige uma correção de emergência e precisa fazer isso em todos os seus ambientes manualmente.

Benefícios de estabelecer esta prática recomendada: Ao estabelecer um processo de gerenciamento de patches, incluindo seus critérios de aplicação de patches e metodologia para distribuição em seus ambientes, você pode escalar e gerar relatórios sobre os níveis de patch. Isso fornece garantias sobre a aplicação de patches de segurança e garante uma visibilidade clara do status das correções

conhecidas em vigor. Isso permite a adoção de recursos e capacidades desejados, a remoção rápida de problemas e a conformidade contínua com a governança. Implemente sistemas de gerenciamento de patches e automação para reduzir o nível de esforço na implantação de patches e limitar erros causados por processos manuais.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Aplice patches nos sistemas para corrigir problemas, obter os recursos ou capacidades desejados e permanecer em conformidade com a política de governança e os requisitos de suporte do fornecedor. Em sistemas imutáveis, implante com o conjunto de patches adequado para alcançar o resultado desejado. Automatize o mecanismo de gerenciamento de patches para reduzir o tempo decorrido na aplicação de patches, reduzir erros causados por processos manuais e reduzir o nível de esforço para corrigir.

Etapas da implementação

Para Amazon EC2 Image Builder:

1. Usando o Amazon EC2 Image Builder, especifique os detalhes do pipeline:
 - a. Crie um pipeline de imagens e dê um nome a ele
 - b. Defina o cronograma e o fuso horário do pipeline
 - c. Configure todas as dependências
2. Escolha uma fórmula:
 - a. Selecione a fórmula existente ou crie uma nova.
 - b. Selecione o tipo de imagem.
 - c. Nomeie e crie a versão da sua fórmula
 - d. Selecione sua imagem base
 - e. Adicione componentes de compilação e adicione ao registro de destino
3. Opcional: defina sua configuração de infraestrutura.
4. Opcional: defina as configurações.
5. Revise as configurações.
6. Mantenha a higiene da fórmula regularmente.

Para o Systems Manager Patch Manager:

1. Crie uma lista de referência de patches.
2. Selecione um método de operações de definição de caminho.
3. Habilite relatórios e escaneamentos de conformidade.

Recursos

Práticas recomendadas relacionadas:

- [OPS06-BP04 Automatizar os testes e a reversão](#)

Documentos relacionados:

- [O que é o Amazon EC2 Image Builder](#)
- [Crie um pipeline de imagens usando o Amazon EC2 Image Builder](#)
- [Crie um pipeline de imagens de contêiner](#)
- [AWS Systems Manager Patch Manager](#)
- [Trabalhar com o Patch Manager](#)
- [Trabalhar com relatórios de conformidade de patches](#)
- [Ferramentas de desenvolvedor da AWS](#)

Vídeos relacionados:

- [CI/CD para aplicações de tecnologia sem servidor na AWS](#)
- [Projeto com Ops em mente](#)

Exemplos relacionados:

- [Laboratórios do Well-Architected: Gerenciamento de inventário e patches](#)
- [Tutoriais do AWS Systems Manager Patch Manager](#)

OPS05-BP06 Compartilhar os padrões de design

Compartilhe as melhores práticas entre as equipes para aumentar a conscientização e maximizar os benefícios dos esforços de desenvolvimento. Documente-as e mantenha-as atualizadas à medida que sua arquitetura evolui. Se forem aplicados padrões compartilhados na sua organização, será

fundamental que haja mecanismos para solicitar adições, alterações e exceções para os padrões. Sem essa opção, os padrões se tornam uma restrição à inovação.

Resultado desejado: padrões de design são compartilhados entre as equipes nas organizações. Eles são documentados e mantidos atualizados de acordo com a evolução das práticas recomendadas.

Antipadrões comuns:

- Cada uma das duas equipes de desenvolvimento criou um serviço de autenticação de usuários. Os usuários devem manter um conjunto separado de credenciais para cada parte do sistema que desejam acessar.
- Cada equipe gerencia sua própria infraestrutura. Um novo requisito de conformidade força uma alteração na infraestrutura e cada equipe o implementa de maneira diferente.

Benefícios de estabelecer esta prática recomendada: o uso dos padrões compartilhados apoia a adoção das práticas recomendadas e maximiza os benefícios dos esforços de desenvolvimento. A documentação e atualização dos padrões de design mantém a organização atualizada com relação às práticas recomendadas e aos requisitos de segurança e conformidade.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Compartilhe as práticas recomendadas, os padrões de design, as listas de verificação, os procedimentos operacionais, as orientações e os requisitos de governança entre equipes. Tenha procedimentos para solicitar alterações, adições e exceções para padrões de design a fim de apoiar a melhoria e a inovação. As equipes devem estar cientes do conteúdo publicado. Tenha um mecanismo para manter os padrões de design atualizados à medida que surgem novas práticas recomendadas.

Exemplo de clientes

A AnyCompany Retail tem uma equipe de arquitetura multifuncional que cria padrões de arquitetura de software. Essa equipe cria a arquitetura com conformidade e governança integradas. As equipes que adotam esses padrões compartilhados recebem os benefícios de ter a conformidade e governança integradas. Elas podem criar rapidamente com base no padrão de design. A equipe de arquitetura se reúne trimestralmente para avaliar os padrões de arquitetura e atualizá-los, se necessário.

Etapas da implementação

1. Identifique uma equipe multifuncional que seja responsável pelo desenvolvimento e pela atualização dos padrões de design. Essa equipe deverá trabalhar com as partes interessadas na organização para desenvolver os padrões de design, os procedimentos operacionais, as listas de verificações, as orientações e os requisitos de governança. Documente os padrões de design e compartilhe-os na organização.
 - a. [O AWS Service Catalog](#) pode ser usado para criar portfólios representando os padrões de design usando infraestrutura como código. É possível compartilhar portfólios entre contas.
2. Tenha um mecanismo em vigor para manter os padrões de design atualizados à medida que novas práticas recomendadas são identificadas.
3. Se os padrões de design forem aplicados centralmente, tenha um processo para solicitar alterações, atualizações e isenções.

Nível de esforço do plano de implementação: médio. O desenvolvimento de um processo para criar e compartilhar padrões de design pode exigir coordenação e cooperação com as partes interessadas na organização.

Recursos

Práticas recomendadas relacionadas:

- [OPS01-BP03 Avaliar os requisitos de governança](#) – Os requisitos de governança influenciam os padrões de design.
- [OPS01-BP04 Avaliar os requisitos de conformidade](#) – A conformidade é um fator fundamental na criação dos padrões de design.
- [OPS07-BP02 Garantir uma análise consistente da prontidão operacional](#) – As listas de verificação de prontidão operacional são um mecanismo para implementar os padrões de design ao projetar a workload.
- [OPS11-BP01 Ter um processo para a melhoria contínua](#) – A atualização dos padrões de design faz parte da melhoria contínua.
- [OPS11-BP04 Realizar o gerenciamento de conhecimento](#) – Como parte da sua prática de gerenciamento de conhecimento, documente e compartilhe os padrões de design.

Documentos relacionados:

- [Automatizar AWS Backups com AWS Service Catalog](#)
- [Conta do AWS Service Catalog aprimorada para o setor](#)
- [Como o Expedia Group criou uma oferta de banco de dados como serviço \(DBaaS\) usando o AWS Service Catalog](#)
- [Manter a visibilidade sobre o uso dos padrões de arquitetura de nuvem](#)
- [Simplifique o compartilhamento de seus portfólios do AWS Service Catalog em uma configuração do AWS Organizations](#)

Vídeos relacionados:

- [AWS Service Catalog – conceitos básicos](#)
- [AWS re:Invent 2020: gerencie seus portfólios do AWS Service Catalog como especialista](#)

Exemplos relacionados:

- [Arquitetura de referência do AWS Service Catalog](#)
- [Workshop do AWS Service Catalog](#)

Serviços relacionados:

- [AWS Service Catalog](#)

OPS05-BP07 Implementar práticas para aprimorar a qualidade do código

Implemente práticas para aprimorar a qualidade do código e minimizar os defeitos. Alguns exemplos incluem desenvolvimento orientado por testes, análises de código, adoção de padrões e programação de pares. Incorpore essas práticas em seu processo de entrega e integração contínua.

Resultado desejado: Sua organização usa práticas recomendadas como análises de código ou programação de pares para melhorar a qualidade do código. Os desenvolvedores e operadores adotam práticas recomendadas de qualidade do código como parte do ciclo de vida de desenvolvimento de software.

Antipadrões comuns:

- Você confirma o código para a ramificação principal da aplicação sem uma análise de código. A alteração é implantada automaticamente na produção e causa uma interrupção.
- Uma nova aplicação é desenvolvida sem nenhum teste de integração, completo ou de unidade. Não há como testar a aplicação antes da implantação.
- Sua equipe faz alterações manuais na produção para solucionar os defeitos. As alterações não passam por testes ou análises de código e não são capturadas nem registradas por processos contínuos de entrega e integração.

Benefícios de estabelecer esta prática recomendada: Ao adotar práticas para melhorar a qualidade do código, é possível reduzir os problemas surgidos na produção. A qualidade do código aumenta com o uso de práticas recomendadas como programação de pares e análises de código.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Implemente práticas para melhorar a qualidade do código visando a minimizar os defeitos antes que eles sejam implantados. Use práticas como desenvolvimento orientado por testes, análises de código e programação de pares para aumentar a qualidade do desenvolvimento.

Exemplo de clientes

A AnyCompany Retail adota várias práticas para melhorar a qualidade do código. O desenvolvimento orientado por testes foi adotado como padrão para escrever aplicações. Para alguns recursos novos, os desenvolvedores fazem a programação em pares durante um sprint. Cada pull request passa por uma análise de código feita por um desenvolvedor sênior antes de ser integrada e implantada.

Etapas da implementação

1. Adote práticas de qualidade de código como desenvolvimento orientado por testes, análises de código e programação de pares em seu processo de entrega e integração contínua. Use essas técnicas para melhorar a qualidade do software.
 - a. [O Amazon CodeGuru Reviewer](#) pode fornecer recomendações de programação para código Java e Python usando machine learning.
 - b. Você pode criar ambientes de desenvolvimento compartilhados com o [AWS Cloud9](#), onde você pode colaborar no desenvolvimento de código.

Nível de esforço do plano de implementação: Médio. Há muitas maneiras de implementar essa prática recomendada, mas pode ser difícil garantir a adesão organizacional.

Recursos

Práticas recomendadas relacionadas:

- [OPS05-BP06 Compartilhar os padrões de design](#) – É possível compartilhar padrões de design como parte de sua prática de qualidade de código.

Documentos relacionados:

- [Agile Software Guide \(Guia do software Agile\)](#)
- [My CI/CD pipeline is my release captain \(Meu pipeline de CI/CD é meu capitão de lançamentos\)](#)
- [Análises de código automatizadas com o Amazon CodeGuru Reviewer](#)
- [Adopt a test-driven development approach \(Adotar uma abordagem de desenvolvimento orientada a testes\)](#)
- [How DevFactory builds better applications with Amazon CodeGuru \(Como o DevFactory cria melhores aplicações com o Amazon CodeGuru\)](#)
- [On Pair Programming \(Sobre a programação de pares\)](#)
- [RENGA Inc. automates code reviews with Amazon CodeGuru \(RENGA Inc. automatiza análises de código com o Amazon CodeGuru\)](#)
- [The Art of Agile Development: Test-Driven Development \(A arte do desenvolvimento ágil: desenvolvimento orientado por testes\)](#)
- [Why code reviews matter \(and actually save time!\) \(Por que as análises de código são importantes \(e economizam tempo!\)\)](#)

Vídeos relacionados:

- [AWS re:Invent 2020: Continuous improvement of code quality with Amazon CodeGuru \(AWS re:Invent 2020: melhoria contínua da qualidade do código com o Amazon CodeGuru\)](#)
- [AWS Summit ANZ 2021 - Driving a test-first strategy with CDK and test driven development \(AWS Summit ANZ 2021: conduzir uma estratégia de primeiro teste com o CDK e desenvolvimento orientado a testes\)](#)

Serviços relacionados:

- [Amazon CodeGuru Reviewer](#)
- [Amazon CodeGuru Profiler](#)
- [AWS Cloud9](#),

OPS05-BP08 Usar vários ambientes

Use vários ambientes para experimentar, desenvolver e testar a workload. Use níveis crescentes de controles à medida que os ambientes se aproximam da produção para adquirir confiança de que sua workload operará conforme pretendido quando implantada.

Resultado desejado: Você tem vários ambientes que refletem suas necessidades de conformidade e governança. Você testa e promove o código por meio de ambientes em seu caminho para a produção.

Antipadrões comuns:

- Você está realizando o desenvolvimento em um ambiente de desenvolvimento compartilhado e outro desenvolvedor substitui suas alterações de código.
- Os controles de segurança restritivos em seu ambiente de desenvolvimento compartilhado estão impedindo que você experimente novos serviços e recursos.
- Você realiza testes de carga em seus sistemas de produção e causa uma interrupção para seus usuários.
- Ocorreu um erro crítico na produção que resulta na perda de dados. No ambiente de produção, você tenta recriar as condições que levaram à perda de dados para identificar como isso aconteceu e impedir a recorrência. Para evitar mais perda de dados durante o teste, você é forçado a tornar indisponível a aplicação para seus usuários.
- Você está operando um serviço multilocatário e não consegue oferecer suporte a uma solicitação do cliente para um ambiente dedicado.
- Nem sempre você testa, mas, quando o faz, o teste acontece em seu ambiente de produção.
- Você acredita que a simplicidade de um único ambiente substitui o escopo do impacto das alterações dentro do ambiente.

Benefícios de estabelecer esta prática recomendada: Você pode oferecer suporte a vários ambientes simultâneos de desenvolvimento, teste e produção, sem criar conflitos entre desenvolvedores ou comunidades de usuários.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Use vários ambientes e forneça aos desenvolvedores ambientes de sandbox com controles minimizados para permitir a experimentação. Forneça ambientes de desenvolvimento individuais para ajudar o trabalho em paralelo, aumentando a agilidade do desenvolvimento. Implemente controles mais rigorosos nos ambientes ao se aproximar da produção para permitir que os desenvolvedores inovem. Use a infraestrutura como sistemas de gerenciamento de código e configuração para implantar ambientes que são configurados de maneira consistente com os controles presentes na produção para garantir que os sistemas operem conforme o esperado quando implantados. Quando os ambientes não estiverem em uso, desligue-os para evitar custos associados a recursos inativos (por exemplo, sistemas de desenvolvimento à noite e fins de semana). Implante ambientes equivalentes de produção ao carregar o teste para melhorar resultados válidos.

Recursos

Documentos relacionados:

- [Programador de instâncias na AWS](#)
- [O que é o AWS CloudFormation?](#)

OPS05-BP09 Fazer alterações frequentes, pequenas e reversíveis

Alterações frequentes, pequenas e reversíveis reduzem o escopo e o impacto de uma alteração. Quando usadas em conjunto com sistemas de gerenciamento de mudanças, sistemas de gerenciamento de configuração e sistemas de compilação e entrega, mudanças frequentes, pequenas e reversíveis reduzem o escopo e o impacto de uma mudança. Isso resulta em solução de problemas mais eficaz e correção mais rápida, com a opção de reverter alterações.

Antipadrões comuns:

- Você implanta uma nova versão de sua aplicação trimestralmente com uma janela de alteração que significa que um serviço principal está desativado.

- Você frequentemente faz alterações no esquema do banco de dados sem rastrear as alterações nos sistemas de gerenciamento.
- Você realiza atualizações manuais no local, substituindo as instalações e configurações existentes e não tem um plano claro de reversão.

Benefícios de estabelecer esta prática recomendada: Os esforços de desenvolvimento são mais rápidos com a implantação frequente de pequenas mudanças. Quando as alterações são pequenas, é muito mais fácil identificar se elas têm consequências indesejadas e são mais fáceis de serem revertidas. Quando as alterações são reversíveis, há menos risco de implementar a alteração à medida que a recuperação é simplificada. O processo de mudança tem um risco reduzido e o impacto de uma alteração malsucedida é reduzido.

Nível de risco exposto se esta prática recomendada não for estabelecida: Baixo

Orientação para implementação

Use alterações frequentes, pequenas e reversíveis para reduzir o escopo e o impacto de uma alteração. Isso facilita a solução de problemas, ajuda a fazer uma correção mais rápida e oferece a opção de reverter uma alteração. Também aumenta a taxa na qual você pode agregar valor aos negócios.

Recursos

Práticas recomendadas relacionadas:

- [OPS05-BP03 Usar sistemas de gerenciamento de configuração](#)
- [OPS05-BP04 Usar sistemas de gerenciamento de compilação e de implantação](#)
- [OPS06-BP04 Automatizar os testes e a reversão](#)

Documentos relacionados:

- [Implementing Microservices on AWS \(Implementação de microsserviços na AWS\)](#)
- [Microservices - Observability \(Microsserviços: observabilidade\)](#)

OPS05-BP10 Automatizar totalmente a integração e a implantação

Automatize a construção, implantação e o teste da workload. Isso reduz os erros causados pelos processos manuais e reduz o esforço para implantar alterações.

Aplique metadados usando o [Tags de recursos](#) e [AWS Resource Groups](#) seguindo uma estratégia [consistente de marcação](#) para permitir a identificação dos seus recursos. Identifique seus recursos de organização, contabilidade de custos, controles de acesso pensando na execução de atividades operacionais automatizadas.

Resultado desejado: os desenvolvedores usam ferramentas para entregar códigos e levá-los até a produção. Os desenvolvedores não precisam fazer login no AWS Management Console para fazer atualizações. Há uma trilha de auditoria completa de alterações e configurações, atendendo às necessidades de governança e conformidade. Os processos são repetíveis e padronizados entre as equipes. Os desenvolvedores podem se concentrar no desenvolvimento e na introdução de código, aumentando a produtividade.

Antipadrões comuns:

- Na sexta-feira, você conclui a criação do novo código para a ramificação do recurso. Na segunda-feira, depois de executar os scripts de teste de qualidade de código e cada um dos scripts de teste de unidade, você registra seu código para a próxima versão programada.
- Você tem a tarefa de codificar uma correção para um problema crítico que afeta um grande número de clientes em produção. Depois de testar a correção, você confirma o gerenciamento de alterações de e-mail e código para solicitar aprovação para implantá-lo na produção.
- Como desenvolvedor, você faz login no AWS Management Console para criar um novo ambiente de desenvolvimento usando métodos e sistemas que não são padrão.

Benefícios de estabelecer esta prática recomendada: ao implementar sistemas automatizados de gerenciamento de criação e implantação, você reduz os erros causados por processos manuais e o esforço para implantar alterações, ajudando os membros da equipe a se concentrarem na entrega de valor para a empresa. Você aumenta a velocidade de entrega à medida que avança até a produção.

Nível de risco exposto se esta prática recomendada não for estabelecida: Baixo

Orientação para implementação

Você usa sistemas de gerenciamento de criação e implantação para rastrear e implementar alterações, reduzir erros causados por processos manuais e reduzir o nível de esforço. Automatize

totalmente o pipeline de integração e implantação desde o check-in do código até a compilação, o teste, a implantação e a validação. Isso reduz o tempo de espera, aumenta a frequência de alterações, reduz o nível de esforço, aumenta a velocidade de entrada no mercado, resulta em maior produtividade e aumenta a segurança do seu código à medida que você o leva até a produção.

Recursos

Práticas recomendadas relacionadas:

- [OPS05-BP03 Usar sistemas de gerenciamento de configuração](#)
- [OPS05-BP04 Usar sistemas de gerenciamento de compilação e de implantação](#)

Documentos relacionados:

- [O que é o AWS CodeBuild?](#)
- [O que é o AWS CodeDeploy?](#)

Vídeos relacionados:

- [AWS re\Invent 2022 - AWS Well-Architected best practices for DevOps on AWS](#)

Mitigar riscos de implantação

Adote abordagens que forneçam feedback rápido sobre a qualidade e permitam recuperação rápida de alterações que não têm os resultados desejados. O uso dessas práticas reduz o impacto dos problemas introduzidos pela implantação de mudanças.

O projeto da sua workload deve incluir como ela será implantada, atualizada e operada. Você deseja implementar práticas de engenharia alinhadas com a redução de defeitos e correções rápidas e seguras.

Práticas recomendadas

- [OPS06-BP01 Preparar-se para alterações malsucedidas](#)
- [OPS06-BP02 Testar as implantações](#)
- [OPS06-BP03 Utilizar estratégias de implantação seguras](#)
- [OPS06-BP04 Automatizar os testes e a reversão](#)

OPS06-BP01 Preparar-se para alterações malsucedidas

Planeje reverter para um bom estado anterior ou realize reparos no ambiente de produção se a implantação causar um resultado indesejado. Ter uma política para estabelecer esse plano ajuda todas as equipes a desenvolver estratégias para se recuperar de alterações com falha. Alguns exemplos de estratégias são etapas de implantação e reversão, políticas de alteração, sinalizadores de atributos, isolamento de tráfego e mudança de tráfego. Uma única versão pode incluir várias alterações de componentes relacionadas. A estratégia deve fornecer a possibilidade de resistir ou se recuperar de uma falha de qualquer alteração de componente.

Resultado desejado: Você preparou um plano de recuperação detalhado para a alteração, caso ela não tenha êxito. Além disso, você reduziu o tamanho da sua versão para minimizar o impacto potencial em outros componentes da workload. Como resultado, você reduziu o impacto nos negócios ao diminuir o possível tempo de inatividade decorrente de uma alteração malsucedida e aumentou a flexibilidade e a eficiência dos tempos de recuperação.

Antipadrões comuns:

- Você executou uma implantação e seu aplicativo se tornou instável, mas parece haver usuários ativos no sistema. Você precisa decidir se deseja reverter a alteração e afetar os usuários ativos ou esperar para reverter a alteração sabendo que, mesmo assim, os usuários podem ser afetados.
- Depois de fazer uma alteração de rotina, os novos ambientes ficam acessíveis, mas uma de suas sub-redes se tornou inacessível. Você precisa decidir se deseja reverter tudo ou tentar corrigir a sub-rede inacessível. Enquanto você estiver fazendo essa determinação, a sub-rede permanecerá inacessível.
- Seus sistemas não são arquitetados de uma forma que permite que sejam atualizados com versões menores. Como resultado, você tem dificuldade em reverter essas alterações em massa durante uma implantação com falha.
- Você não usa a infraestrutura como código (IaC) e foram feitas atualizações manuais nela que resultaram em uma configuração indesejada. Você não consegue rastrear e reverter com eficácia as alterações manuais.
- Como você não mediu o aumento da frequência das implantações, sua equipe não é incentivada a reduzir o tamanho das mudanças e melhorar seus planos de reversão para cada uma delas, gerando mais riscos e maiores taxas de falha.
- Você não mede a duração total de uma interrupção causada por alterações malsucedidas. A equipe não consegue priorizar e melhorar a eficácia do processo de implantação e do plano de recuperação.

Benefícios de estabelecer esta prática recomendada: Ter um plano para se recuperar de mudanças malsucedidas minimiza o tempo médio de recuperação (MTTR) e reduz o impacto nos negócios.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

A adoção de uma política e prática documentadas e consistentes por parte das equipes de lançamento permitem que a organização planeje o que deve ocorrer se houver mudanças malsucedidas. A política deve permitir a correção em circunstâncias específicas. Seja qual for a situação, um plano de correção antecipada ou reversão deve ser bem documentado e testado antes da implantação na produção em tempo real, a fim de que o tempo necessário para reverter uma alteração seja minimizado.

Etapas da implementação

1. Documente as políticas que exigem que as equipes tenham planos efetivos para reverter as mudanças dentro de um período especificado.
 - a. As políticas devem especificar quando uma situação de correção antecipada é permitida.
 - b. Exija que um plano de reversão documentado seja acessível a todos os envolvidos.
 - c. Especifique os requisitos de reversão (por exemplo, quando for constatado que foram implantadas alterações não autorizadas).
2. Analise o nível de impacto de todas as mudanças relacionadas a cada componente de uma workload.
 - a. Permita que alterações repetíveis sejam padronizadas, modeladas e pré-autorizadas se seguirem um fluxo de trabalho consistente que imponha políticas de mudança.
 - b. Reduza o impacto potencial de qualquer alteração diminuindo o tamanho dela para que a recuperação leve menos tempo e cause um impacto menor nos negócios.
 - c. Garanta que os procedimentos de reversão revertam o código para um bom estado conhecido a fim de evitar incidentes sempre que possível.
3. Integre ferramentas e fluxos de trabalho para aplicar suas políticas de forma programática.
4. Torne os dados sobre as alterações visíveis para outros proprietários da workload a fim de melhorar a velocidade do diagnóstico de qualquer alteração malsucedida que não possa ser revertida.
 - a. Avalie o sucesso dessa prática usando dados de mudança visíveis e identifique melhorias iterativas.

5. Use ferramentas de monitoramento para verificar o sucesso ou a falha de uma implantação a fim de acelerar a tomada de decisões sobre a reversão.
6. Meça a duração da interrupção durante uma alteração malsucedida para melhorar continuamente seus planos de recuperação.

Nível de esforço do plano de implementação: médio

Recursos

Práticas recomendadas relacionadas:

- [OPS06-BP04 Automatizar os testes e a reversão](#)

Documentos relacionados:

- [AWS Builders Library | Ensuring Rollback Safety During Deployments](#)
- [Whitepaper da AWS | Change Management in the Cloud](#)

Vídeos relacionados:

- [re:Invent 2019 | A abordagem da Amazon para implantação de alta disponibilidade](#)

OPS06-BP02 Testar as implantações

Teste os procedimentos de lançamento na pré-produção usando a mesma configuração de implantação, controles de segurança, etapas e procedimentos da produção. Valide se todas as etapas implantadas foram concluídas conforme o esperado, como inspecionar arquivos, configurações e serviços. Teste ainda mais todas as alterações com testes funcionais, de integração e de carga, além de qualquer monitoramento, como verificações de integridade. Ao fazer esses testes, você pode identificar problemas de implantação com antecedência, podendo planejá-los e mitigá-los antes da produção.

Você pode criar ambientes paralelos temporários para testar cada alteração. Automatize a implantação dos ambientes de teste usando a infraestrutura como código (IaC) para ajudar a reduzir a quantidade de trabalho envolvido e garantir estabilidade, consistência e entrega mais rápida de atributos.

Resultado desejado: A organização adota uma cultura de desenvolvimento orientada a testes que inclui testes de implantações. Isso garante que as equipes se concentrem em oferecer valor empresarial em vez de gerenciar lançamentos. As equipes são engajadas desde o início após a identificação dos riscos de implantação para determinar o curso apropriado da mitigação.

Antipadrões comuns:

- Durante as versões de produção, implantações não testadas causam problemas frequentes que exigem soluções e encaminhamento.
- Sua versão contém infraestrutura como código (IaC) que atualiza os recursos existentes. Você não tem certeza se a IaC será executada com êxito ou causará impacto nos recursos.
- Você implanta um novo atributo na aplicação. Ele não funciona conforme o esperado e não há visibilidade até ser relatado pelos usuários afetados.
- Você atualiza seus certificados. Você instala acidentalmente os certificados nos componentes errados, o que não é detectado e afeta os visitantes do site porque não é possível estabelecer uma conexão segura.

Benefícios de estabelecer esta prática recomendada: Testes extensivos na pré-produção dos procedimentos de implantação, considerando-se que as mudanças introduzidas por eles minimizam o impacto potencial na produção causado pelas etapas de implantação. Isso aumenta a confiança durante o lançamento da produção e minimiza o suporte operacional sem diminuir a velocidade das alterações que estão sendo entregues.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

Testar seu processo de implantação é tão importante quanto testar as alterações resultantes da implantação. Isso pode ser realizado testando suas etapas de implantação em um ambiente de pré-produção que se assemelhe o máximo possível à produção. Problemas comuns, como etapas de implantação incompletas ou incorretas, ou configurações incorretas, podem ser detectados como resultado antes da produção. Além disso, você pode testar suas etapas de recuperação.

Exemplo de clientes

Como parte do pipeline de integração e entrega contínuas (CI/CD), a Loja UmaEmpresa executa as etapas definidas necessárias para lançar atualizações de infraestrutura e software para seus clientes em um ambiente semelhante ao de produção. O pipeline é composto por pré-verificações

para detectar desvios (detecção de alterações nos recursos executados fora da IaC) nos recursos antes da implantação, bem como validar as ações que a IaC realiza após seu início. Ele valida as etapas de implantação, como verificar se determinados arquivos e configurações estão em vigor e se os serviços estão em execução e respondendo corretamente às verificações de integridade no host local antes de serem registrados novamente no balanceador de carga. Além disso, todas as alterações sinalizam vários testes automatizados, como testes funcionais, de segurança, de regressão, de integração e de carga.

Etapas para a implementação

1. Execute verificações de pré-instalação para espelhar o ambiente de pré-produção na produção.
 - a. Use [detecção de desvios](#) para detectar quando os recursos foram alterados fora do AWS CloudFormation.
 - b. Use [conjuntos de alterações](#) para validar se a intenção da atualização da pilha corresponde às ações que o AWS CloudFormation realiza quando o conjunto de alterações é iniciado.
2. Isso aciona uma etapa de aprovação manual no [AWS CodePipeline](#) para autorizar a implantação no ambiente de pré-produção.
3. Use configurações de implantação, como [arquivos do AWS CodeDeploy AppSpec](#) para definir as etapas de implantação e validação.
4. Quando aplicável, [integre o AWS CodeDeploy a outros serviços da AWS](#) ou [integre o AWS CodeDeploy a produtos e serviços de parceiros](#).
5. [Monitore as implantações](#) usando notificações de eventos do Amazon CloudWatch, do AWS CloudTrail e do Amazon SNS.
6. Execute testes automatizados pós-implantação, incluindo testes funcionais, de segurança, regressão, integração e carga.
7. [Solução de problemas](#) de implantação.
8. A validação bem-sucedida das etapas acima deve iniciar um fluxo de trabalho de aprovação manual para autorizar a implantação na produção.

Nível de esforço do plano de implementação: Alto

Recursos

Práticas recomendadas relacionadas:

- [OPS05-BP02 Testar e valide as alterações](#)

Documentos relacionados:

- [AWS Builders' Li| Automating safe, hands-off deployments | Test Deployments](#)
- [Whitepaper da AWS Whitepaper | Practicing Continuous Integration and Continuous Delivery on AWS](#)
- [A história da Apollo: o mecanismo de implantação da Amazon](#)
- [How to test and debug AWS CodeDeploy locally before you ship your code](#)
- [Integrar testes de conectividade de rede com implantação de infraestrutura](#)

Vídeos relacionados:

- [re:Invent 2020 | Testar software e sistemas na Amazon](#)

Exemplos relacionados:

- [Tutorial | Deploy and Amazon ECS service with a validation test](#)

OPS06-BP03 Utilizar estratégias de implantação seguras

Implantações seguras de produção controlam o fluxo de mudanças benéficas com o objetivo de minimizar qualquer impacto percebido dessas alterações para os clientes. Os controles de segurança fornecem mecanismos de inspeção para validar os resultados desejados e limitar o escopo do impacto dos defeitos introduzidos pelas alterações ou das falhas de implantação. As implementações seguras podem incluir estratégias como sinalizadores de atributos e implantações one-box, contínuas (versões canário), imutáveis, de divisão de tráfego e azuis/verdes.

Resultado desejado: sua organização usa um sistema de integração e entrega contínuas (CI/CD) que fornece recursos para automatizar implementações seguras. As equipes devem usar estratégias apropriadas de implantação seguras.

Antipadrões comuns:

- Você implanta uma alteração malsucedida em toda a produção de uma só vez. Como resultado, todos os clientes são afetados simultaneamente.
- Um defeito introduzido em uma implantação simultânea em todos os sistemas requer um lançamento de emergência. A correção para todos os clientes leva vários dias.

- O gerenciamento da versão de produção requer planejamento e participação de várias equipes. Isso restringe sua capacidade de atualizar atributos com frequência para seus clientes.
- Você executa uma implantação mutável modificando os sistemas existentes. Depois de descobrir que a alteração não foi bem-sucedida, você será forçado a modificar os sistemas novamente para restaurar a versão antiga, aumentando o seu tempo de recuperação.

Benefícios de estabelecer esta prática recomendada: implantações automatizadas equilibram a velocidade das implementações com a entrega consistente de mudanças benéficas aos clientes. Limitar o impacto evita falhas de implantação dispendiosas e maximiza a capacidade das equipes de responder às falhas de forma eficiente.

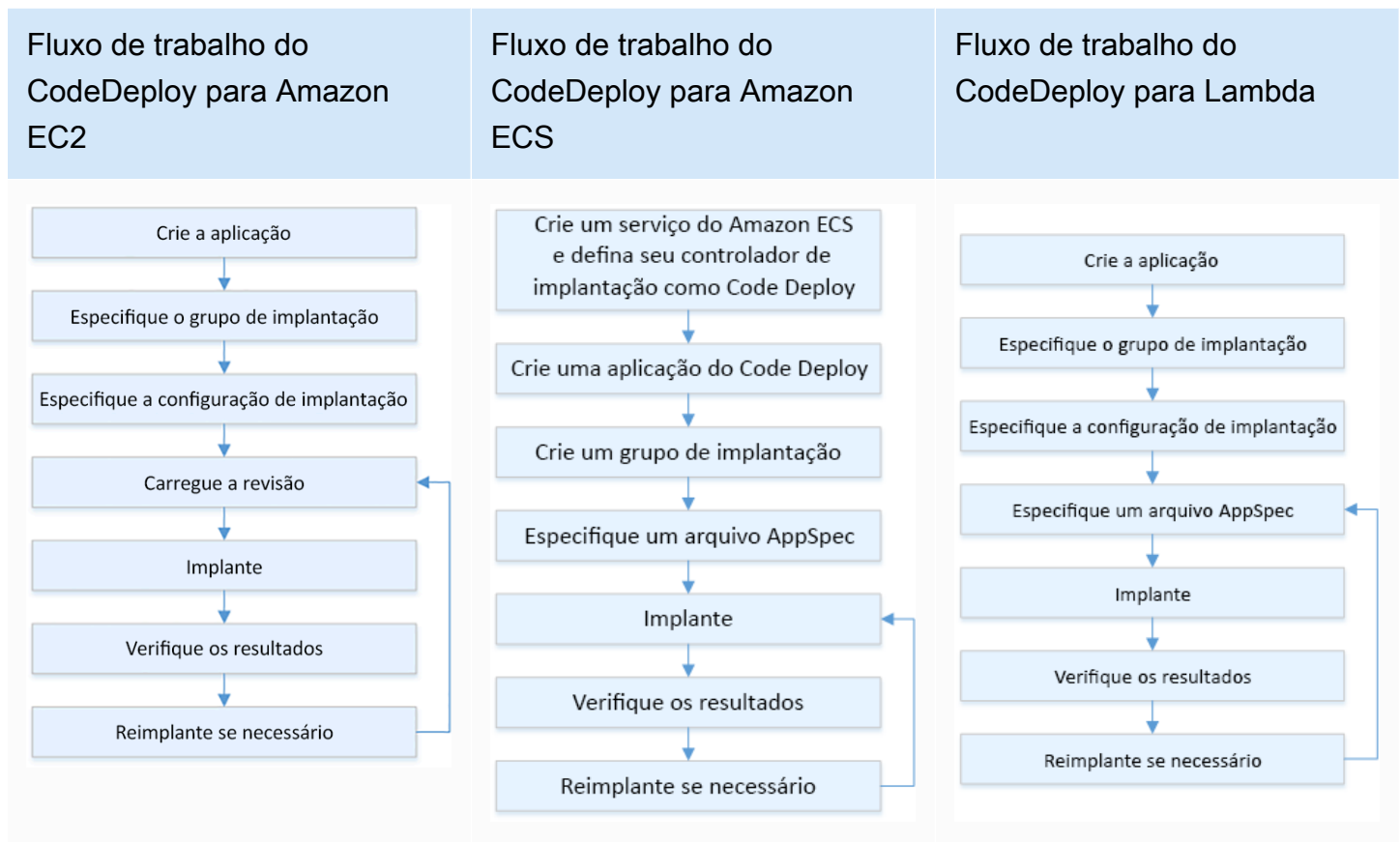
Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Falhas na entrega contínua podem levar à redução da disponibilidade do serviço e a uma experiência ruim para o cliente. Para maximizar a taxa de implantações bem-sucedidas, implemente controles de segurança no processo de lançamento de ponta a ponta para minimizar os erros de implantação e eliminar as falhas.

Exemplo de clientes

A Loja UmaEmpresa tem a missão de alcançar implantações com tempo de inatividade entre mínimo e zero, isto é, sem impacto perceptível para seus usuários durante as implantações. Para fazer isso, a empresa estabeleceu padrões de implantação (consulte o diagrama de fluxo de trabalho a seguir), como implantações azuis/verdes e contínuas. Todas as equipes adotam um ou mais desses padrões no pipeline de CI/CD.



Etapas da implementação

1. Use um fluxo de trabalho de aprovação para iniciar a sequência das etapas de implantação na promoção para implantação.
2. Use um sistema de implantação automatizado, como o [AWS CodeDeploy](#). As opções de implantação do AWS CodeDeploy incluem implantações locais do EC2/on-premises e implantações azuis/verdes do EC2/on-premises, do AWS Lambda e do Amazon ECS (consulte o diagrama de fluxo de trabalho anterior).
 - a. Quando aplicável, [integre o AWS CodeDeploy a outros serviços da AWS](#) ou [integre o AWS CodeDeploy a produtos e serviços de parceiros](#).
3. Use implantações azuis/verdes para bancos de dados, como [Amazon Aurora](#) e o [Amazon RDS](#).
4. [Monitore as implantações](#) usando notificações de eventos do Amazon CloudWatch, do AWS CloudTrail e do Amazon SNS.
5. Realize testes automatizados pós-implantação, incluindo testes funcionais, de segurança, regressão, integração e testes de carga.
6. [Solução de problemas](#) de implantação.

Nível de esforço do plano de implementação: médio

Recursos

Práticas recomendadas relacionadas:

- [OPS05-BP02 Testar e valide as alterações](#)
- [OPS05-BP09 Fazer alterações frequentes, pequenas e reversíveis](#)
- [OPS05-BP10 Automatizar totalmente a integração e a implantação](#)

Documentos relacionados:

- [AWS Builders Library | Automating safe, hands-off deployments | Production deployments](#)
- [AWS Builders Library | My CI/CD pipeline is my release captain | Safe, automatic production releases](#)
- [Whitepaper da AWS | Practicing Continuous Integration and Continuous Delivery on AWS | Deployment methods](#)
- [Guia do usuário do AWS CodeDeploy](#)
- [Working with deployment configurations in AWS CodeDeploy](#)
- [Set up an API Gateway canary release deployment](#)
- [Amazon ECS Deployment Types](#)
- [Fully Managed Blue/Green Deployments in Amazon Aurora and Amazon RDS](#)
- [Blue/Green deployments with AWS Elastic Beanstalk](#)

Vídeos relacionados:

- [re:Invent 2020 | Sem intervenção manual: como automatizar os pipelines de entrega contínua na Amazon](#)
- [re:Invent 2019 | A abordagem da Amazon para implantação de alta disponibilidade](#)

Exemplos relacionados:

- [Try a Sample Blue/Green Deployment in AWS CodeDeploy](#)
- [Workshop | Buiding CI/CD pipelines for Lambda canary deployments using AWS CDK](#)

- [Workshop | Implantação canário e azul/verde para o EKS e o ECS](#)
- [Workshop | Criar um pipeline de CI/CD entre contas](#)

OPS06-BP04 Automatizar os testes e a reversão

Para aumentar a velocidade, a confiabilidade e a confiança do seu processo de implantação, tenha uma estratégia para testes automatizados e recursos de reversão em ambientes de pré-produção e produção. Automatize os testes ao implantar na produção para simular interações entre humanos e sistemas que verifiquem as alterações que estão sendo implantadas. Automatize a reversão para voltar rapidamente a um estado anterior em boas condições. A reversão deve ser iniciada automaticamente em condições predefinidas, como quando o resultado desejado da alteração não é alcançado ou quando o teste automatizado falha. A automação dessas duas atividades melhora a taxa de sucesso das implantações, minimiza o tempo de recuperação e reduz o impacto potencial nos negócios.

Resultado desejado: Os testes automatizados e as estratégias de reversão são integrados ao pipeline de integração e entrega contínuas (CI/CD). O monitoramento é capaz de validar seus critérios de sucesso e iniciar a reversão automática em caso de falha. Isso minimiza qualquer impacto para usuários finais e clientes. Por exemplo, quando todos os resultados do teste são satisfatórios, você promove seu código no ambiente de produção em que o teste de regressão automatizado é iniciado, utilizando os mesmos casos de teste. Se os resultados do teste de regressão não corresponderem às expectativas, a reversão automática será iniciada no fluxo de trabalho do pipeline.

Antipadrões comuns:

- Seus sistemas não são arquitetados de uma forma que permite que sejam atualizados com versões menores. Como resultado, você tem dificuldade em reverter essas alterações em massa durante uma implantação com falha.
- O processo de implantação consiste em uma série de etapas manuais. Depois de implantar as alterações na workload, você inicia os testes pós-implantação. Após o teste, você percebe que a workload está inoperante e os clientes estão desconectados. Em seguida, você começa a reverter para a versão anterior. Todas essas etapas manuais atrasam a recuperação geral do sistema e causam um impacto prolongado para os clientes.
- Você passou um tempo desenvolvendo casos de teste automatizados para funcionalidades que não são usadas com frequência na aplicação, minimizando o retorno sobre o investimento no recurso de teste automatizado.

- Sua versão é composta de atualizações de aplicações, infraestrutura, patches e configuração que são independentes umas das outras. No entanto, você tem um único pipeline de CI/CD que fornece todas as alterações de uma só vez. Uma falha em um componente força você a reverter todas as alterações, tornando a reversão complexa e ineficiente.
- A equipe conclui o trabalho de codificação no primeiro sprint e inicia o trabalho no segundo sprint, mas seu plano não incluiu testes até o terceiro sprint. Como resultado, os testes automatizados revelaram defeitos do primeiro sprint que precisavam ser resolvidos antes que o teste dos resultados do segundo sprint pudesse ser iniciado, adiando todo o lançamento e desvalorizando seus testes automatizados.
- Seus casos de teste de regressão automatizados para a versão de produção estão completos, mas você não está monitorando a integridade da workload. Como você não tem visibilidade sobre se o serviço foi reiniciado, você não tem certeza se a reversão é necessária ou se ela já ocorreu.

Benefícios de estabelecer esta prática recomendada: O teste automatizado aumenta a transparência do processo de teste e a capacidade de abranger mais atributos em um período mais curto. Ao testar e validar as mudanças na produção, você pode identificar problemas imediatamente. A melhoria na consistência com ferramentas de teste automatizadas permite uma melhor detecção de defeitos. Ao reverter automaticamente para a versão anterior, o impacto sobre seus clientes é minimizado. A reversão automatizada acaba inspirando mais confiança em seus recursos de implantação ao reduzir o impacto nos negócios. No geral, esses recursos reduzem o tempo de entrega e, ao mesmo tempo, garantem a qualidade.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Automatize os testes dos ambientes implantados para confirmar os resultados desejados mais rapidamente. Automatize a reversão para um bom estado anterior conhecido quando os resultados predefinidos não forem alcançados, para minimizar o tempo de recuperação e reduzir os erros causados por processos manuais. Integre ferramentas de teste com seu fluxo de trabalho de pipeline para testar e minimizar as entradas manuais de forma consistente. Priorize a automação de casos de teste, como aqueles que mitigam os maiores riscos e precisam ser testados com frequência a cada alteração. Além disso, automatize a reversão com base em condições específicas predefinidas no plano de teste.

Etapas para a implementação

1. Estabeleça um ciclo de vida de teste para o ciclo de vida de desenvolvimento que defina cada estágio do processo de teste, desde o planejamento dos requisitos até o desenvolvimento do caso de teste, a configuração da ferramenta, o teste automatizado e o encerramento do caso de teste.
 - a. Crie uma abordagem de teste específica para workloads com base em sua estratégia geral de teste.
 - b. Considere uma estratégia de teste contínuo, quando apropriado, durante o ciclo de vida do desenvolvimento.
2. Selecione ferramentas automatizadas para testes e reversões com base em seus requisitos de negócios e investimentos em pipeline.
3. Decida quais casos de teste você deseja automatizar e quais deverão ser executados manualmente. Eles podem ser definidos com base na prioridade do valor comercial do atributo que está sendo testado. Alinhe todos os membros da equipe a esse plano e verifique a responsabilidade pela realização de testes manuais.
 - a. Aplique recursos de teste automatizados a casos de teste específicos que façam sentido para automação, como casos repetíveis ou executados com frequência, aqueles que exigem tarefas repetitivas ou aqueles que são necessários em várias configurações.
 - b. Defina scripts de automação de testes, bem como os critérios de sucesso na ferramenta de automação, para que a automação contínua do fluxo de trabalho possa ser iniciada quando casos específicos falharem.
 - c. Defina critérios de falha específicos para a reversão automatizada.
4. Priorize a automação de testes para gerar resultados consistentes com o desenvolvimento completo de casos de teste em que a complexidade e a interação humana têm um risco maior de falha.
5. Integre as ferramentas automatizadas de teste e reversão no pipeline de CI/CD.
 - a. Desenvolva critérios claros de sucesso para as alterações.
 - b. Monitore e observe para detectar esses critérios e reverter automaticamente as alterações quando critérios específicos de reversão forem atendidos.
6. Execute diferentes tipos de teste de produção automatizados, como:
 - a. Teste A/B para mostrar resultados em comparação com a versão atual entre dois grupos de teste de usuários.
 - b. Teste canário, que permite implantar a alteração em um subconjunto de usuários antes de lançá-la para todos.

- c. Teste de sinalização de atributos, que permite que a sinalização de um único atributo da nova versão seja ativada e desativada de fora da aplicação para que cada novo atributo possa ser validado individualmente.
 - d. Teste de regressão para verificar novas funcionalidades com componentes inter-relacionados existentes.
7. Monitore os aspectos operacionais da aplicação, das transações e das interações com outras aplicações e componentes. Desenvolva relatórios para mostrar o sucesso das alterações por workload e identificar quais partes da automação e do fluxo de trabalho podem ser ainda mais otimizadas.
- a. Desenvolva relatórios de resultados de testes que ajudem você a tomar decisões rápidas sobre se os procedimentos de reversão devem ou não ser invocados.
 - b. Implemente uma estratégia que permita a reversão automatizada com base em condições de falha predefinidas que resultam de um ou mais de seus métodos de teste.
8. Desenvolva seus casos de teste automatizados para permitir a reutilização em futuras alterações repetíveis.

Nível de esforço do plano de implementação: médio

Recursos

Práticas recomendadas relacionadas:

- [OPS06-BP01 Preparar-se para alterações malsucedidas](#)
- [OPS06-BP02 Testar as implantações](#)

Documentos relacionados:

- [AWS Builders Library | Ensuring rollback safety during deployments](#)
- [Redeploy and rollback a deployment with AWS CodeDeploy](#)
- [8 best practices when automating your deployments with AWS CloudFormation](#)

Exemplos relacionados:

- [Serverless UI testing using Selenium, AWS Lambda, AWS Fargate \(Fargate\), and AWS Developer Tools](#)

Vídeos relacionados:

- [re:Invent 2020 | Sem intervenção manual: como automatizar os pipelines de entrega contínua na Amazon](#)
- [re:Invent 2019 | A abordagem da Amazon para implantação de alta disponibilidade](#)

Prontidão operacional e gerenciamento de alterações

Avalie a prontidão operacional de workload, processos, procedimentos e pessoal para compreender os riscos operacionais relacionados à workload. Gerencie o fluxo de alterações em seus ambientes.

Você deve usar um processo consistente (incluindo listas de verificação manuais ou automatizadas) para saber quando está pronto para trabalhar com sua workload ou para fazer uma mudança. Isso também ajudará a encontrar as áreas que você precisa abordar. Você terá runbooks que documentam suas atividades de rotina e manuais operacionais que orientam seus processos para a resolução de problemas. Use um mecanismo para gerenciar alterações que apoie a entrega de valor empresarial e ajude a mitigar riscos associados a mudanças.

Práticas recomendadas

- [OPS07-BP01 Garantir a capacidade da equipe](#)
- [OPS07-BP02 Garantir uma análise consistente da prontidão operacional](#)
- [OPS07-BP03 Usar runbooks para realizar procedimentos](#)
- [OPS07-BP04 Usar manuais para investigar problemas](#)
- [OPS07-BP05 Tomar decisões embasadas para implantar sistemas e alterações](#)
- [OPS07-BP06 Viabilizar planos de suporte para workloads de produção](#)

OPS07-BP01 Garantir a capacidade da equipe

Tenha um mecanismo para validar que você tem o número adequado de funcionários treinados para fornecer suporte à workload. Eles devem ter treinamento para a plataforma e os serviços que compõem sua workload. Forneça a eles o conhecimento necessário para operar a workload. É necessário ter o número suficiente de funcionários treinados para fornecer suporte à operação da workload e solucionar os incidentes que ocorrerem. Tenha funcionários suficientes para que seja possível alterná-los durante plantões e férias, a fim de evitar a exaustão.

Resultado desejado:

- Há um número suficiente de funcionários treinados para fornecer suporte à workload quando a workload estiver disponível.
- Você fornece treinamento para seus funcionários sobre software e serviços que compõem a workload.

Antipadrões comuns:

- Implantar uma workload sem membros da equipe treinados para operar a plataforma e os serviços em uso.
- Não ter funcionários suficientes para fornecer suporte à alternâncias de plantão ou folga de funcionários.

Benefícios do estabelecimento desta prática recomendada:

- Ter membros da equipe qualificados possibilita o suporte eficaz da sua carga de trabalho.
- Com um número suficiente de membros na equipe, é possível dar conta da workload e das alternâncias de plantão, reduzindo o risco de exaustão.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

Valide se há um número suficiente de funcionários treinados para fornecer suporte à workload. Verifique se você tem membros da equipe suficientes para cobrir as atividades operacionais normais, incluindo alternâncias de plantão.

Exemplo de clientes

A Loja UmaEmpresa garante que as equipes que fornecem suporte à workload estejam completas e treinadas. Há engenheiros suficientes para fornecer suporte a uma alternância de plantão. Os funcionários têm treinamento referente ao software e à plataforma na qual a workload é criada e são incentivados a obter certificações. Há funcionários suficientes para que as pessoas possam tirar folgas enquanto mantêm o suporte à workload e à alternância de plantões.

Etapas da implementação

1. Atribua um número adequado de funcionários para operar e fornecer suporte à workload, incluindo tarefas de plantão.

2. Treine seus funcionários referente ao software e às plataformas que compõem a workload.
 - a. O [AWS Training and Certification](#) tem uma biblioteca de cursos sobre a AWS. Estão disponíveis cursos pagos e gratuitos, online e presenciais.
 - b. [A AWS promove eventos e webinars](#) por meio dos quais você aprende com especialistas da AWS.
3. Avalie regularmente o tamanho e as habilidades da equipe à medida que as condições operacionais e a workload mudam. Ajuste o tamanho e as habilidades da equipe para corresponderem aos requisitos operacionais.

Nível de esforço do plano de implementação: alto. Contratar e treinar uma equipe para fornecer suporte a uma workload pode exigir um esforço significativo, mas traz benefícios substanciais de longo prazo.

Recursos

Práticas recomendadas relacionadas:

- [OPS11-BP04 Realizar o gerenciamento de conhecimento](#) – Os membros da equipe devem ter as informações necessárias para operar e fornecer suporte à workload. O gerenciamento de conhecimento é fundamental para fornecer isso.

Documentos relacionados:

- [Eventos e webinars da AWS](#)
- [AWS Training and Certification](#)

OPS07-BP02 Garantir uma análise consistente da prontidão operacional

Use Análises de prontidão operacional (ORRs) para validar que você pode operar sua workload. A ORR é um mecanismo desenvolvido na Amazon para validar que as equipes podem operar as workloads com segurança. Uma ORR é um processo de análise e inspeção que usa uma lista de verificação de requisitos. Uma ORR é uma experiência de autoatendimento que as equipes usam para certificar suas workloads. As ORRs incluem práticas recomendadas de lições aprendidas de nossos anos de experiência na criação de software.

Uma lista de verificação de ORR é composta de recomendações de arquitetura, processo operacional, gerenciamento de evento e qualidade de lançamento. Nosso processo de Correção

de erros (CoE) é um motivador principal desses itens. Sua própria análise pós-incidente deve impulsionar a evolução de sua própria ORR. Uma ORR não é apenas sobre seguir as práticas recomendadas, mas evitar a recorrência de eventos que você já viu. Por fim, os requisitos de segurança, governança e conformidade também podem ser incluídos em uma ORR.

Execute ORRs antes do lançamento de uma workload para disponibilidade geral e por todo o ciclo de vida de desenvolvimento do software. A execução da ORR antes do lançamento aumenta a capacidade de operar a workload com segurança. Execute a ORR periodicamente na workload para identificar qualquer desvio das práticas recomendadas. Você pode ter listas de verificação da ORR para o lançamento de outros serviços e ORRs para avaliações periódicas. Isso ajuda a manter você atualizado sobre as novas práticas recomendadas que surgem e incorporar as lições aprendidas da análise pós-incidente. À medida que seu uso da nuvem amadurece, é possível criar requisitos de ORR em sua arquitetura como padrões.

Resultado desejado: você tem uma lista de verificação da ORR com as práticas recomendadas para sua organização. As ORRs são realizadas antes do lançamento das workloads. As ORRs são executadas periodicamente ao longo do ciclo de vida da workload.

Antipadrões comuns:

- Você lança uma workload sem saber se pode operá-la.
- Os requisitos de governança e segurança não estão incluídos na certificação de uma workload para o lançamento.
- As workloads não são reavaliadas periodicamente.
- As workloads são lançadas sem a aplicação dos procedimentos exigidos.
- Você vê a repetição das mesmas falhas da causa raiz em várias workloads.

Benefícios de estabelecer esta prática recomendada:

- suas workloads incluem práticas recomendadas de arquitetura, processo e gerenciamento.
- As lições aprendidas são incorporadas em seu processo de ORR.
- Os procedimentos exigidos estão em vigor no lançamento das workloads.
- As ORRs são executadas durante todo o ciclo de vida do software das workloads.

Nível de risco caso essa prática recomendada não seja estabelecida: alto

Orientação para implementação

Uma ORR é composta por dois elementos: um processo e uma lista de verificação. O processo da ORR deve ser adotado pela organização e ter o apoio de um patrocinador executivo. No mínimo, as ORRs devem ser realizadas antes do lançamento da workload para disponibilidade geral. Execute a ORR ao longo de todo o ciclo de vida de desenvolvimento do software para mantê-la atualizada com as práticas recomendadas ou os novos requisitos. A lista de verificação da ORR deve incluir itens de configuração, requisitos de segurança e governança e práticas recomendadas de sua organização. Ao longo do tempo, você pode usar serviços como o [AWS Config](#), o [AWS Security Hub](#) e o [AWS Control Tower Guardrails](#), para criar práticas recomendadas com base na ORR visando as barreiras de proteção para detecção automática das práticas recomendadas.

Exemplo de cliente

Depois de vários incidentes na produção, a Loja UmaEmpresa decidiu implementar um processo de ORR. Ela criou uma lista de verificação composta de práticas recomendadas, requisitos de governança e conformidade e lições aprendidas de interrupções. Novas workloads passam pelo processo de ORR antes do lançamento. É realizada uma ORR anualmente para cada workload com um subconjunto de práticas recomendadas a incorporar novas práticas recomendadas e requisitos que são adicionados à lista de verificação da ORR. Ao longo do tempo, a Loja UmaEmpresa usou o [AWS Config](#) para detectar algumas práticas recomendadas, acelerando o processo de ORR.

Etapas da implementação

Para saber mais sobre as ORRs, leia o [whitepaper de Análises de prontidão operacional \(ORR\)](#). Ele fornece informações detalhadas sobre o histórico do processo de ORR, como criar sua própria prática de ORR e como desenvolver sua lista de verificação da ORR. As etapas a seguir são uma versão resumida desse documento. Para uma compreensão aprofundada do que são as ORRs e de como criar sua própria, recomendamos a leitura desse whitepaper.

1. Reúna as principais partes interessadas, incluindo os representantes de segurança, operações e desenvolvimento.
2. Peça para cada parte interessada fornecer pelo menos um requisito. Para a primeira iteração, tente limitar o número de itens para trinta ou menos.
 - [Apêndice B: os exemplos de perguntas da ORR](#) do whitepaper de Análises de prontidão operacional (ORR) contém exemplos de perguntas que você pode usar para começar.
3. Reúna seus requisitos em uma planilha.

- Você pode usar o [Custom Lenses](#) no [AWS Well-Architected Tool](#) para desenvolver sua ORR e compartilhá-la em suas contas e no AWS Organization.
4. Identifique uma workload na qual realizar a ORR. O ideal seria em uma workload em pré-lançamento ou uma workload interna.
 5. Execute a lista de verificação completa da ORR e anote as descobertas feitas. As descobertas podem não ser corretas caso esteja ocorrendo uma mitigação. Para descobertas que não tenham uma mitigação, acrescente-as à sua lista de pendências e implemente-as antes do lançamento.
 6. Continue a adicionar práticas recomendadas e requisitos à sua lista de verificação de ORR ao longo do tempo.

Os clientes do AWS Support com Enterprise Support podem solicitar o [workshop de Análises de prontidão operacional](#) com seu gerente de conta técnico. O workshop é uma sessão interativa de trabalho em retrospecto para que você consiga desenvolver sua própria lista de verificação de ORR.

Nível de esforço do plano de implementação: alto. Adotar uma prática de ORR em sua organização exige a adesão de um patrocinador executivo e das partes interessadas. Crie e atualize a lista de verificação com as opiniões de toda a sua organização.

Recursos

Práticas recomendadas relacionadas:

- [OPS01-BP03 Avaliar os requisitos de governança](#) – Os requisitos de governança são uma opção natural para uma lista de verificação da ORR.
- [OPS01-BP04 Avaliar os requisitos de conformidade](#) – Os requisitos de conformidade, às vezes são incluídos em uma lista de verificação de ORR. Outras vezes, eles constituem um processo separado.
- [OPS03-BP07 Fornecer recursos adequados às equipes](#) – A capacidade da equipe é uma boa candidata para um requisito de ORR.
- [OPS06-BP01 Preparar-se para alterações malsucedidas](#) – Um plano de reversão ou avanço deve ser estabelecido antes do lançamento da workload.
- [OPS07-BP01 Garantir a capacidade da equipe](#) – Para comportar uma workload, você deve ter o pessoal necessário.
- [SEC01-BP03 Identificar e validar objetivos de controle](#) – Os objetivos de controle de segurança compõem excelentes requisitos de ORR.

- [REL13-BP01 Definir os objetivos de recuperação para tempo de inatividade e perda de dados](#) – Os planos de recuperação de desastres são um ótimo requisito de ORR.
- [COST02-BP01 Desenvolver políticas com base nos requisitos da sua organização](#) – As políticas de gerenciamento de custos são ótimas para incluir em sua lista de verificação de ORR.

Documentos relacionados:

- [AWS Control Tower - Guardrails in AWS Control Tower \(AWS Control Tower: barreiras de proteção no AWS Control Tower\)](#)
- [AWS Well-Architected Tool - Custom Lenses](#)
- [Operational Readiness Review Template by Adrian Hornsby \(Modelo de Análise de prontidão operacional, por Adrian Hornsby\)](#)
- [Whitepaper de Análises de prontidão operacional \(ORR\)](#)

Vídeos relacionados:

- [AWS Supports You | Building an Effective Operational Readiness Review \(ORR\) \(Apoio do AWS Support: criação de uma Análise de prontidão operacional \(ORR\) eficaz\)](#)

Exemplos relacionados:

- [Sample Operational Readiness Review \(ORR\) Lens \(Exemplo da perspectiva da Análise de prontidão operacional \(ORR\)\)](#)

Serviços relacionados:

- [AWS Config](#)
- [AWS Control Tower](#)
- [AWS Security Hub](#)
- [AWS Well-Architected Tool](#)

OPS07-BP03 Usar runbooks para realizar procedimentos

A runbook é um processo documentado para alcançar um resultado específico. Runbooks consistem em uma série de etapas que alguém segue para realizar alguma coisa. Runbooks são usados

em operações desde os primórdios da aviação. Nas operações na nuvem, usamos runbooks para reduzir o risco e alcançar os resultados desejados. Em essência, um runbook é uma lista de verificação para concluir uma tarefa.

Runbooks são fundamentais para a operação de uma workload. Da integração de um novo membro da equipe à implantação de um lançamento importante, os runbooks são os processos codificados que fornecem resultados consistentes independentemente de quem os usa. Os runbooks devem estar publicados em um local central e devem ser atualizados à medida que o processo evolui, uma vez que a atualização dos runbooks é um aspecto fundamental de um processo de gerenciamento de mudanças. Também devem incluir orientação sobre tratamento de erros, ferramentas, permissões, exceções e encaminhamentos em caso de problema.

À medida que sua organização amadurece, comece a automatizar os runbooks. Comece com runbooks que sejam curtos e usados com frequência. Use linguagens de scripts para automatizar as etapas ou facilitar a realização delas. À medida que você automatiza os primeiros runbooks, vai dedicar tempo à automação de runbooks mais complexos. Com o tempo, a maioria dos seus runbooks deverão ter algum nível de automação.

Resultado desejado: sua equipe tem um conjunto de guias detalhados para realizar tarefas de workload. Os runbooks contêm o resultado desejado, as ferramentas e permissões necessárias e as instruções para tratamento de erros. Eles estão armazenados em um local central e são atualizados frequentemente.

Antipadrões comuns:

- Dependendo da memória para concluir cada etapa de um processo.
- Implantar mudanças manualmente sem uma lista de verificação.
- Vários membros da equipe realizando o mesmo processo, mas com etapas ou resultados diferentes.
- Deixar que os runbooks fiquem desatualizados em relação às mudanças no sistema e à automação.

Benefícios do estabelecimento desta prática recomendada:

- Redução das taxas de erros em tarefas manuais.
- Operações realizadas de maneira consistente.
- Novos membros da equipe podem começar a realizar tarefas mais cedo.

- Os runbooks podem ser automatizados para reduzir o esforço.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação de implementação

Os runbooks podem assumir diversos formatos dependendo do nível de maturidade da sua organização. No mínimo, devem consistir em um documento de texto detalhado. O resultado desejado deve estar claramente identificado. Documentar claramente as permissões ou ferramentas especiais necessárias. Fornecer orientação detalhada sobre tratamento de erros e encaminhamentos em caso de problema. Listar o proprietário do runbook e publicá-lo em um local central. Depois que o runbook estiver documentado, valide-o pedindo que outro membro da equipe o execute. À medida que os procedimentos evoluem, atualize os runbooks de acordo com seu processo de gerenciamento de mudanças.

Os runbooks em texto devem ser automatizados à medida que a organização amadurece. Usando serviços como as [automações do AWS Systems Manager](#), você pode transformar texto plano em automações que podem ser executadas na workload. Essas automações podem ser executadas em resposta a eventos, reduzindo a sobrecarga operacional de manutenção da workload.

Exemplo de cliente

A AnyCompany Retail precisa realizar atualizações no esquema de banco de dados durante implantações de software. A equipe de operações na nuvem trabalhou com a equipe de administração do banco de dados para criar um runbook para implantação manual dessas mudanças. O runbook lista cada etapa do processo em um formato de lista de verificação. Ele inclui uma seção sobre tratamento de erros em caso de problema. Eles publicaram o runbook na wiki interna junto com outros runbooks. A equipe de operações na nuvem planeja automatizar o runbook em um sprint futuro.

Etapas da implementação

Se você não tem um repositório de documentos, um repositório de controle de versão é um ótimo lugar para começar a criar sua biblioteca de runbooks. Você pode criar runbooks usando Markdown. Disponibilizamos um modelo de runbook que você pode usar para começar a criar runbooks.

```
# Título do runbook ## Informações do runbook | ID do runbook | Descrição | Ferramentas
usadas | Permissões especiais | Criador do runbook | Última atualização | Contato para
encaminhamento | |-----|-----|-----|-----|-----|-----|-----| | RUN001 |
```


Para que serve este runbook? Qual é o resultado desejado? | Ferramentas | Permissões
| Seu nome | 21-09-2022 | Nome para encaminhamento | ## Etapas 1. Primeira etapa 2.
Segunda etapa

1. Se você não tiver um repositório de documentação ou uma wiki, crie um repositório de controle de versão em seu sistema de controle de versão.
2. Identifique um processo que não tenha um runbook. Um processo ideal é um que seja realizado quase regularmente, que tenha poucas etapas e que tenha falhas de baixo impacto.
3. No repositório de documentos, crie um rascunho de documento em Markdown usando o modelo. Preencha `Título do runbook` e os campos necessários em `Informações do runbook`.
4. Começando pela primeira etapa, preencha a seção `Etapas` do runbook.
5. Dê o runbook a um membro da equipe. Peça que o use para validar as etapas. Se algo estiver faltando ou não estiver claro, atualize o runbook.
6. Disponibilize o runbook em seu armazenamento interno de documentos. Depois, informe a sua equipe e outras partes interessadas.
7. Com o passar do tempo, você terá uma biblioteca de runbooks. À medida que essa biblioteca cresce, comece a trabalhar na automatização dos runbooks.

Nível de esforço do plano de implementação: baixo. O padrão mínimo para um runbook é um guia de texto detalhado. A automatização dos runbooks pode aumentar o esforço de implementação.

Recursos

Práticas recomendadas relacionadas:

- [OPS02-BP02 Processos e procedimentos com proprietários identificados](#): os runbooks devem ter um proprietário responsável por mantê-los.
- [OPS07-BP04 Usar manuais para investigar problemas](#): os runbooks e playbooks são semelhantes, com uma diferença importante: um runbook tem um resultado desejado. Em muitos casos, os runbooks são acionados depois que um playbook identifica uma causa raiz.
- [OPS10-BP01 Usar um processo para gerenciamento de eventos, incidentes e problemas](#): os runbooks fazem parte de uma boa prática de gerenciamento de eventos, incidentes e problemas.
- [OPS10-BP02 Ter um processo por alerta](#): os runbooks e playbooks devem ser usados para responder a alertas. Com o tempo, essas reações devem ser automatizadas.
- [OPS11-BP04 Realizar o gerenciamento de conhecimento](#): a manutenção dos runbooks é essencial para o gerenciamento de conhecimento.

Documentos relacionados:

- [Como alcançar excelência operacional usando playbooks e runbooks automatizados](#)
- [AWS Systems Manager: trabalhar com runbooks](#)
- [Playbook para grandes migrações da AWS - Tarefa 4: Como melhorar runbooks de migração](#)
- [Como usar runbooks do AWS Systems Manager Automation para resolver tarefas operacionais](#)

Vídeos relacionados:

- [AWS re:Invent 2019: DIY guide to runbooks, incident reports, and incident response \(SEC318-R1\) \(Guia DIY para runbooks, relatórios de incidentes e resposta a incidentes\)](#)
- [How to automate IT Operations on AWS | Amazon Web Services \(Como automatizar operações de TI na AWS | Amazon Web Services\)](#)
- [Integrate Scripts into AWS Systems Manager \(Integração de scripts no AWS Systems Manager\)](#)

Exemplos relacionados:

- [AWS Systems Manager: demonstrações de automação](#)
- [AWS Systems Manager: runbook para restaurar um volume raiz usando o snapshot mais recente](#)
- [Criar um runbook de resposta a incidentes da AWS usando cadernos Jupyter e CloudTrail Lake](#)
- [Gitlab: runbooks](#)
- [Rubix: uma biblioteca de Python para criação de runbooks em cadernos Jupyter](#)
- [Como usar o gerador de documentos para criar um runbook personalizado](#)
- [Well-Architected Labs: automatização de operações com playbooks e runbooks](#)

Serviços relacionados:

- [AWS Systems Manager Automation](#)

OPS07-BP04 Usar manuais para investigar problemas

Os manuais são guias detalhados usados para investigar incidentes. Quando incidentes ocorrem, os manuais são usados para investigar, definir o escopo do impacto e identificar a causa raiz. Os manuais são usados em diversos cenários, desde falhas em implantações até incidentes de

segurança. Em muitos casos, os manuais identificam a causa raiz mitigada por um runbook. Os manuais são essenciais aos planos de resposta a incidentes de sua organização.

Um bom manual abrange vários aspectos principais. Ele guia o usuário, detalhadamente, ao longo do processo de descoberta. Considerando várias perspectivas, quais etapas devem ser seguidas para diagnosticar um incidente? Defina claramente no manual se são necessárias ferramentas especiais ou permissões elevadas. Ter um plano de comunicação para atualizar as partes interessadas sobre o status da investigação é essencial. Em situações em que a causa raiz ainda não foi identificada, o manual deve ter um plano de escalação. Se a causa raiz tiver sido identificada, o manual deverá indicar um runbook que descreva como resolvê-la. Os manuais devem ser armazenados em um local central e atualizados com frequência. Caso os manuais sejam usados para alertas específicos, forneça às equipes indicadores para o manual no alerta.

À medida que sua organização for amadurecendo, automatize seus manuais. Comece com manuais que abordem incidentes de baixo risco. Use scripts para automatizar as etapas de descoberta. Tenha runbooks complementares para mitigar as causas raízes comuns.

Resultado desejado: Sua organização tem manuais para incidentes comuns. Os manuais são armazenados em um local central e estão disponíveis para os membros da equipe. Os manuais são atualizados com frequência. São criados runbooks complementares para todas as causas raízes conhecidas.

Antipadrões comuns:

- Não há uma maneira padrão de investigar um incidente.
- Os membros da equipe precisam confiar na própria memória ou no conhecimento institucional para solucionar uma falha na implantação.
- Os novos membros da equipe aprendem a investigar os problemas por meio de tentativa e erro.
- As práticas recomendadas para a investigação dos problemas não são compartilhadas entre as equipes.

Benefícios de estabelecer esta prática recomendada:

- Os manuais impulsionam seus esforços para mitigar os incidentes.
- Diferentes membros da equipe podem usar o mesmo manual para identificar uma causa raiz de maneira consistente.
- As causas raízes conhecidas podem ter runbooks desenvolvidos para elas, o que acelera o tempo de recuperação.

- Os manuais permitem que os membros da equipe comecem a contribuir o quanto antes.
- As equipes podem escalar seus processos com manuais repetíveis.

Nível de risco exposto se essa prática recomendada não for estabelecida: Médio

Orientação para implementação

A maneira que você cria e usa os manuais depende da maturidade de sua organização. Se você é iniciante na nuvem, crie manuais no formato de texto em um repositório central de documentos. À medida que sua organização amadurecer, os manuais poderão passar a ser semiautomatizados com linguagens de script, como Python. Esses scripts podem ser executados em um caderno Jupyter para acelerar a descoberta. As organizações avançadas têm manuais totalmente automatizados para problemas comuns que são corrigidos automaticamente com runbooks.

Comece a criar seus manuais listando incidentes comuns que ocorrem com sua workload. Para começar, escolha manuais para incidentes com baixo risco e nos quais a causa raiz tenha sido restrita a poucos problemas. Quando você tiver manuais para os cenários mais simples, passe para cenários de alto risco ou cenários em que a causa raiz não seja bem conhecida.

Seus manuais em texto deverão ser automatizados à medida que sua organização amadurecer. Usando serviços, como o [AWS Systems Manager Automations](#), um texto sem formatação pode ser transformado em automações. Essas automações podem ser executadas em sua workload para acelerar as investigações. Elas podem ser ativadas em resposta a eventos, o que reduz o tempo necessário para descobrir e resolver incidentes.

Os clientes podem usar o [AWS Systems Manager Incident Manager](#) para responder a incidentes. Esse serviço fornece uma interface única para fazer a triagem de incidentes, informar as partes interessadas durante a descoberta e a mitigação e colaborar durante todo o incidente. Ele usa o AWS Systems Manager Automations para acelerar a detecção e a recuperação.

Exemplo de cliente

Um incidente na produção afetou a Loja UmaEmpresa. O engenheiro de plantão usou um manual para investigar o problema. À medida que foi avançando pelas etapas, ele manteve atualizadas as principais partes interessadas, identificadas no manual. O engenheiro identificou a causa raiz como uma condição de corrida em um serviço de back-end. Usando um runbook, o engenheiro reiniciou o serviço, colocando a Loja UmaEmpresa online novamente.

Etapas da implementação

Se você não tem um repositório de documentos, sugerimos criar um repositório de controle de versão para a biblioteca do manual. É possível criar os manuais usando o Markdown, que é compatível com a maioria dos sistemas de automação de manuais. Se você estiver iniciando do zero, use o modelo de exemplo de manual a seguir.

```
# Título do manual ## Informações do manual | ID do manual | Descrição |
Ferramentas usadas | Permissões especiais | Autor do manual | Última atualização
| Ponto de contato de escalação | Partes interessadas | Plano de comunicação |
|-----|-----|-----|-----|-----|-----|-----|-----|-----| | RUN001 |
Para que é este manual? Ele é usado para qual incidente? | Ferramentas | Permissões
| Seu nome | 21/9/2022 | Nome para escalação | Nome da parte interessada | Como as
atualizações serão comunicadas durante a investigação? | ## Etapas 1. Etapa um 2.
Etapa dois
```

1. Se você não tiver um repositório de documentos ou uma wiki, crie um repositório de controle de versão para seus manuais no sistema de controle de versão.
2. Identifique um problema comum que requer investigação. Ele deve ser um cenário em que a causa raiz esteja limitada a poucos problemas e a resolução seja de baixo risco.
3. Usando o modelo do Markdown, preencha a seção Nome do manual e os campos em Informações do manual.
4. Preencha as etapas de resolução de problemas. Seja o mais claro possível sobre quais ações devem ser executadas ou quais áreas devem ser investigadas.
5. Dê o manual a um membro da equipe e peça para essa pessoa analisá-lo a fim de validá-lo. Caso algo esteja faltando ou não esteja claro, atualize o manual.
6. Publique o manual no repositório de documentos e informe sua equipe e as partes interessadas.
7. Essa biblioteca de manuais crescerá à medida que você adicionar outros manuais. Quando você tiver vários manuais, comece a automatizá-los usando ferramentas como o AWS Systems Manager Automations a fim de manter a automação e os manuais sincronizados.

Nível de esforço do plano de implementação: Baixo. Os manuais devem ser documentos de texto armazenados em um local central. Organizações mais consolidadas passarão a automatizar os respectivos manuais.

Recursos

Práticas recomendadas relacionadas:

- [OPS02-BP02 Processos e procedimentos com proprietários identificados](#): os manuais devem ter um proprietário responsável por mantê-los.
- [OPS07-BP03 Usar runbooks para realizar procedimentos](#): os runbooks e os manuais são semelhantes, com uma diferença importante: um runbook tem um resultado desejado. Em muitos casos, os runbooks são usados quando um manual identifica uma causa raiz.
- [OPS10-BP01 Usar um processo para gerenciamento de eventos, incidentes e problemas](#): os manuais fazem parte de uma boa prática de gerenciamento de eventos, incidentes e problemas.
- [OPS10-BP02 Ter um processo por alerta](#): os runbooks e manuais devem ser usados para responder a alertas. Com o tempo, essas reações devem ser automatizadas.
- [OPS11-BP04 Realizar o gerenciamento de conhecimento](#): a manutenção dos manuais é essencial para o gerenciamento de conhecimento.

Documentos relacionados:

- [Achieving Operational Excellence using automated playbook and runbook \(Como alcançar excelência operacional usando manuais e runbooks automatizados\)](#)
- [AWS Systems Manager: Working with runbooks \(AWS Systems Manager: trabalho com runbooks\)](#)
- [Use AWS Systems Manager Automation runbooks to resolve operational tasks \(Usar runbooks do AWS Systems Manager Automation para resolver tarefas operacionais\)](#)

Vídeos relacionados:

- [AWS re:Invent 2019: DIY guide to runbooks, incident reports, and incident response \(SEC318-R1\) \(Guia DIY para runbooks, relatórios de incidentes e resposta a incidentes\)](#)
- [AWS Systems Manager Incident Manager - AWS Virtual Workshops \(AWS Systems Manager Incident Manager - workshops virtuais da AWS\)](#)
- [Integrate Scripts into AWS Systems Manager \(Integração de scripts no AWS Systems Manager\)](#)

Exemplos relacionados:

- [AWS Customer Playbook Framework \(Framework do manual do cliente daAWS\)](#)

- [AWS Systems Manager: Automation walkthroughs \(AWS Systems Manager: demonstrações de automação\)](#)
- [Building an AWS incident response runbook using Jupyter notebooks and CloudTrail Lake \(Criar um runbook de resposta a incidentes da AWS usando cadernos Jupyter e o CloudTrail Lake\)](#)
- [Rubix – A Python library for building runbooks in Jupyter Notebooks \(Rubix: uma biblioteca de Python para criação de runbooks em cadernos Jupyter\)](#)
- [Using Document Builder to create a custom runbook \(Como usar o gerador de documentos para criar um runbook personalizado\)](#)
- [Well-Architected Labs: Automating operations with Playbooks and Runbooks \(Well-Architected Labs: automatização de operações com manuais e runbooks\)](#)
- [Well-Architected Labs: Incident response playbook with Jupyter \(Well-Architected Labs: manual de resposta a incidentes com o Jupyter\)](#)

Serviços relacionados:

- [AWS Systems Manager Automation](#)
- [AWS Systems Manager Incident Manager](#)

OPS07-BP05 Tomar decisões embasadas para implantar sistemas e alterações

Há processos em vigor para alterações com e sem êxito feitas na workload. Uma estratégia pre-mortem é um exercício em que uma equipe simula uma falha para desenvolver estratégias de mitigação. Use as estratégias pre-mortem para antecipar falhas e criar procedimentos, quando apropriado. Avalie os benefícios e os riscos de implantar alterações na workload. Verifique se todas as alterações estão em conformidade com a governança.

Resultado desejado:

- Você toma decisões embasadas ao implantar alterações na workload.
- As alterações estão em conformidade com a governança.

Antipadrões comuns:

- Implantar uma alteração em nossa workload sem um processo para lidar com uma implantação com falha.
- Fazer alterações no ambiente de produção que estão fora da conformidade com os requisitos de governança.
- Implantar uma nova versão da workload sem estabelecer uma referência para a utilização de recursos.

Benefícios do estabelecimento desta prática recomendada:

- Você está preparado para alterações sem êxito na workload.
- As alterações na workload estão em conformidade com as políticas de governança.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: baixo

Orientações para a implementação

Use estratégias pre-mortem no desenvolvimento de processos para alterações sem êxito. Documente os processos de alterações sem êxito. Garanta que todas as alterações estejam em conformidade com a governança. Avalie os benefícios e os riscos de implantar alterações na workload.

Exemplo de clientes

A Loja UmaEmpresa realiza estratégias pre-mortem regularmente para validar seus processos de alterações sem êxito. Os processos são documentados em uma Wiki compartilhada e atualizados regularmente. Todas as alterações estão em conformidade com os requisitos de governança.

Etapas da implementação

1. Tome decisões embasadas ao implantar alterações na workload. Estabeleça e revise os critérios de uma implantação bem-sucedida. Desenvolva cenários ou critérios que acionariam a reversão de uma alteração. Pondere os benefícios de implantar alterações considerando os riscos de uma alteração sem êxito.
2. Verifique se todas as alterações estão em conformidade com as políticas de governança.
3. Use estratégias pre-mortem para alterações sem êxito e documente as estratégias de migração. Realize um exercício de simulação para modelar uma alteração sem êxito e validar os procedimentos de reversão.

Nível de esforço do plano de implementação: moderado. Implementar uma prática de estratégias pre-mortem requer coordenação e esforço das partes interessadas na organização.

Recursos

Práticas recomendadas relacionadas:

- [OPS01-BP03 Avaliar os requisitos de governança](#) – Os requisitos de governança são um fator fundamental para determinar se uma alteração deve ser implementada.
- [OPS06-BP01 Preparar-se para alterações malsucedidas](#) – Estabeleça planos para mitigar uma implantação sem êxito e use estratégias pre-mortem para validá-los.
- [OPS06-BP02 Testar as implantações](#) – Toda alteração de software deve ser testada adequadamente antes da implantação para reduzir os defeitos na produção.
- [OPS07-BP01 Garantir a capacidade da equipe](#) – Ter um número suficiente de funcionários treinados para fornecer suporte à workload é essencial para tomar uma decisão embasada quanto à implantação de uma alteração no sistema.

Documentos relacionados:

- [Amazon Web Services: risco e conformidade](#)
- [Modelo de responsabilidade compartilhada da AWS](#)
- [Governance in the Nuvem AWS: The Right Balance Between Agility and Safety](#) (Governança na Nuvem AWS: o equilíbrio certo entre agilidade e segurança)

OPS07-BP06 Viabilizar planos de suporte para workloads de produção

Viabilize o suporte para qualquer software e quaisquer serviços dos quais sua workload de produção dependa. Selecione um nível de suporte apropriado para atender às necessidades de nível de serviço da produção. Planos de suporte para essas dependências são necessários no caso de interrupção de um serviço ou de um problema de software. Documente os planos de suporte e como solicitar suporte para todos os fornecedores de serviços e software. Implemente mecanismos que verifiquem se os pontos de contato do suporte são mantidos atualizados.

Resultado desejado:

- Implemente planos de suporte para software e serviços dos quais as workloads de produção dependem.

- Escolha um plano de suporte apropriado com base nas necessidades de nível de serviço.
- Documente os planos de suporte, os níveis de suporte e como solicitar suporte.

Antipadrões comuns:

- Você não tem nenhum plano de suporte junto a um fornecedor de software essencial. Sua workload é afetada por isso e você não pode fazer nada para agilizar a correção ou obter atualizações em tempo hábil do fornecedor.
- Um desenvolvedor que era o principal ponto de contato com um fornecedor de software deixou a empresa. Você não consegue entrar em contato com o suporte do fornecedor diretamente. Você precisa despendar tempo pesquisando e navegando por sistemas de contato genéricos, aumentando o tempo requerido para responder quando necessário.
- Ocorre uma interrupção na produção relacionada a um fornecedor de software. Não há nenhuma documentação sobre como abrir um caso de suporte.

Benefícios do estabelecimento desta prática recomendada:

- Com o nível de suporte apropriado, você é capaz de obter uma resposta no espaço de tempo requerido para atender a necessidades de nível de serviço.
- Como um cliente com suporte, você pode encaminhar a questão se houver problemas na produção.
- Os fornecedores de software e serviços podem ajudar na resolução de problemas durante um incidente.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: baixo

Orientações para a implementação

Viabilize planos de suporte para qualquer software e quaisquer serviços dos quais sua workload de produção dependa. Estabeleça planos de suporte apropriados para atender a necessidades de nível de serviço. Para clientes da AWS, isso significa habilitar o AWS Business Support ou superior em quaisquer contas em que você tenha workloads de produção. Entre em contato regularmente com os fornecedores de suporte para obter atualizações sobre ofertas, processos e contatos de suporte. Documente como solicitar suporte de fornecedores de software e serviços e sobre como encaminhar problemas se houver uma interrupção. Implemente mecanismos para manter os contatos de suporte atualizados.

Exemplo de clientes

Na Loja UmaEmpresa, todas dependências de software e serviços comerciais contam com planos de suporte. Por exemplo, eles têm o AWS Enterprise Support habilitado em todas as contas com workloads de produção. Qualquer desenvolvedor pode abrir um caso de suporte quando há um problema. Há uma página de wiki com informações sobre como solicitar suporte, a quem notificar e as práticas recomendadas para agilizar um caso.

Etapas da implementação

1. Trabalhe com as partes interessadas em sua organização para identificar fornecedores de software e serviços dos quais sua workload dependa. Documente essas dependências.
2. Determine as necessidades de nível de serviço para sua workload. Selecione um plano de suporte alinhado a elas.
3. Para software e serviços comerciais, estabeleça um plano de suporte com os fornecedores.
 - a. A assinatura do AWS Business Support ou superior para todas as contas de produção fornece um tempo de resposta rápido do AWS Support e é altamente recomendada. Se você não tiver suporte premium, precisará de um plano de ação para lidar com os problemas, o que requer a ajuda do AWS Support. O AWS Support oferece um conjunto de ferramentas e tecnologia, pessoas e programas projetados para ajudar você de forma proativa a otimizar a performance, reduzir custos e inovar com maior rapidez. O AWS Business Support oferece benefícios adicionais, incluindo acesso ao AWS Trusted Advisor e ao AWS Personal Health Dashboard e tempos de resposta mais rápidos.
4. Documente o plano de suporte em sua ferramenta de gerenciamentos de conhecimentos. Inclua como solicitar suporte, a quem notificar se for aberto um caso de suporte e como encaminhar o problema durante um incidente. Uma wiki é um bom mecanismo para possibilitar que todos façam as atualizações necessárias na documentação quando forem informados sobre alterações em processos ou contatos de suporte.

Nível de esforço do plano de implementação: baixo. A maioria dos fornecedores de software e serviços oferece planos de suporte que requerem adesão. Documentar e compartilhar práticas recomendadas no sistema de gerenciamento de conhecimentos garante que sua equipe saiba o que fazer quando houver um problema na produção.

Recursos

Práticas recomendadas relacionadas:

- [OPS02-BP02 Processos e procedimentos com proprietários identificados](#)

Documentos relacionados:

- [AWS Support Plans](#)

Serviços relacionados:

- [AWS Business Support](#)
- [AWS Enterprise Support](#)

Operar

Êxito é a obtenção de resultados comerciais que correspondem às métricas definidas por você. Ao compreender a integridade da carga de trabalho e das operações, você pode identificar quando os resultados organizacionais e comerciais podem ficar em risco, ou estão em risco, e responder adequadamente.

Para ter êxito, você deve ser capaz de:

Tópicos

- [Utilizar a observabilidade da workload](#)
- [Compreensão da integridade operacional](#)
- [Resposta a eventos](#)

Utilizar a observabilidade da workload

Garanta a integridade ideal da workload usando a observabilidade. Utilize métricas, logs e rastreamentos relevantes para obter uma visão abrangente do desempenho de sua workload e resolver problemas com eficiência.

A observabilidade permite que você se concentre em dados significativos e entenda as interações e os resultados da sua workload. Ao se concentrar em informações essenciais e eliminar dados desnecessários, você mantém uma abordagem direta para entender o desempenho da workload.

É essencial não apenas coletar dados, mas também interpretá-los corretamente. Defina linhas de base claras e limites de alerta apropriados e monitore ativamente quaisquer desvios. Uma mudança em uma métrica-chave, especialmente quando correlacionada com outros dados, pode identificar áreas problemáticas específicas.

Com a observabilidade, você está mais bem equipado para prever e enfrentar possíveis desafios, garantindo que sua workload opere sem problemas e atenda às necessidades comerciais.

A AWS oferece ferramentas específicas, como o [Amazon CloudWatch](#) para monitoramento e registro em log, e o [AWS X-Ray](#) para rastreamento distribuído. Esses serviços se integram facilmente a vários recursos da AWS, permitindo a coleta eficiente de dados, configurando alertas com base em limites predefinidos e apresentando dados em painéis para facilitar a interpretação. Ao usar esses insights, você pode tomar decisões bem informadas e baseadas em dados que se alinham às suas metas operacionais.

Práticas recomendadas

- [OPS08-BP01 Analisar métricas de workload](#)
- [OPS08-BP02 Analisar logs de workloads](#)
- [OPS08-BP03 Analisar rastreamentos de workload](#)
- [OPS08-BP04 Criar alertas acionáveis](#)
- [OPS08-BP05 Criar painéis](#)

OPS08-BP01 Analisar métricas de workload

Depois de implementar a telemetria de aplicações, analise regularmente as métricas coletadas. Embora a latência, as solicitações, os erros e a capacidade (ou cotas) forneçam informações sobre o desempenho do sistema, é fundamental priorizar a análise das métricas de resultados comerciais. Isso garante que você esteja tomando decisões orientadas por dados alinhadas aos seus objetivos de negócios.

Resultado desejado: Insights precisos sobre o desempenho da workload que impulsionam decisões baseadas em dados, garantindo o alinhamento com os objetivos de negócios.

Antipadrões comuns:

- Análise das métricas isoladamente, sem considerar seu impacto nos resultados comerciais.
- Confiança excessiva em métricas técnicas e, ao mesmo tempo, marginalização das métricas de negócios.
- Revisão pouco frequente das métricas, perdendo oportunidades de tomada de decisão em tempo real.

Benefícios de estabelecer esta prática recomendada:

- Compreensão aprimorada da correlação entre desempenho técnico e resultados comerciais.
- Processo de tomada de decisão aprimorado baseado em dados em tempo real.
- Identificação proativa e mitigação de problemas antes que eles afetem os resultados comerciais.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Utilize ferramentas como o Amazon CloudWatch para realizar análises métricas. Serviços da AWS como o AWS Cost Anomaly Detection e o Amazon DevOps Guru podem ser usados para detectar anomalias, especialmente quando os limites estáticos são desconhecidos ou quando os padrões de comportamento são mais adequados para a detecção de anomalias.

Etapas da implementação

1. Analise e revise: Analise e interprete regularmente suas métricas de workload.
 - a. Priorize as métricas de resultados comerciais em vez das métricas puramente técnicas.
 - b. Entenda a importância de picos, quedas ou padrões em seus dados.
2. Use o Amazon CloudWatch: Use o Amazon CloudWatch para uma visão centralizada e uma análise aprofundada.
 - a. Configure painéis do CloudWatch para visualizar suas métricas e compará-las ao longo do tempo.
 - b. Use [percentis no CloudWatch](#) para obter uma visão clara da distribuição métrica, o que pode ajudar na definição de SLAs e na compreensão de valores discrepantes.
 - c. Configure o [AWS Cost Anomaly Detection](#) para identificar padrões incomuns sem depender de limites estáticos.
 - d. Implemente [a observabilidade entre contas do CloudWatch](#) para monitorar e solucionar problemas de aplicações que abrangem várias contas em uma região.
 - e. Use [insights métricos do CloudWatch](#) para consultar e analisar dados métricos em contas e regiões, identificando tendências e anomalias.
 - f. Aplique [matemática métrica do CloudWatch](#) para transformar, agregar ou realizar cálculos em suas métricas para obter insights mais profundos.
3. Empregue o Amazon DevOps Guru: Incorpore o [Amazon DevOps Guru](#) por sua detecção de anomalias aprimorada por machine learning para identificar sinais precoces de problemas operacionais em suas aplicações sem servidor e corrigi-los antes que afetem seus clientes.
4. Otimize com base em insights: Tome decisões informadas com base em sua análise métrica para ajustar e melhorar as workloads.

Nível de esforço do plano de implementação: Médio

Recursos

Práticas recomendadas relacionadas:

- [OPS04-BP01 Identificar os indicadores-chave de performance](#)
- [OPS04-BP02 Implementar a telemetria de aplicações](#)

Documentos relacionados:

- [The Wheel Blog - Emphasizing the importance of continually reviewing metrics \(The Wheel Blog: como enfatizar a importância de revisar continuamente as métricas\)](#)
- [Percentile are important \(O percentil é importante\)](#)
- [Using AWS Cost Anomaly Detection \(Uso da AWS Cost Anomaly Detection\)](#)
- [A observabilidade entre contas do CloudWatch](#)
- [Query your metrics with CloudWatch Metrics Insights \(Consulte suas métricas com o CloudWatch Metrics Insights\)](#)

Vídeos relacionados:

- [Enable Cross-Account Observability in Amazon CloudWatch \(Ative a observabilidade entre contas no Amazon CloudWatch\)](#)
- [Introduction to Amazon DevOps Guru \(Introdução ao Amazon DevOps Guru\)](#)
- [Continuously Analyze Metrics using AWS Cost Anomaly Detection \(Analise continuamente as métricas usando o AWS Cost Anomaly Detection\)](#)

Exemplos relacionados:

- [Um workshop de observabilidade](#)
- [Obter insights operacionais com AIOps usando Amazon DevOps Guru](#)

OPS08-BP02 Analisar logs de workloads

Analisar regularmente os logs da workload é essencial para obter uma compreensão mais profunda dos aspectos operacionais de sua aplicação. Ao filtrar, visualizar e interpretar com eficiência os dados de log, você pode otimizar continuamente o desempenho e a segurança das aplicações.

Resultado desejado: Informações ricas sobre o comportamento e as operações da aplicação derivadas de uma análise completa de log, garantindo a detecção e mitigação proativas de problemas.

Antipadrões comuns:

- Negligenciar a análise dos logs até que surja um problema crítico.
- Não usar o conjunto completo de ferramentas disponíveis para análise de logs, perdendo insights essenciais.
- Confiar exclusivamente na revisão manual dos logs, sem aproveitar os recursos de automação e consulta.

Benefícios de estabelecer esta prática recomendada:

- Identificação proativa de gargalos operacionais, ameaças à segurança e outros possíveis problemas.
- Utilização eficiente dos dados de log para otimização contínua da aplicação.
- Compreensão aprimorada do comportamento da aplicação, auxiliando na depuração e solução de problemas.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

[O Amazon CloudWatch Logs](#) é uma ferramenta poderosa para análise de logs. Recursos integrados, como o CloudWatch Logs Insights e Contributor Insights, tornam intuitivo e eficiente o processo de derivação de informações significativas dos logs.

Etapas da implementação

1. Configure o CloudWatch Logs: Configure aplicações e serviços para enviar logs para o CloudWatch Logs.
2. Configure o CloudWatch Logs Insights: Use o [CloudWatch Logs Insights](#) para pesquisar e analisar interativamente seus dados de log.
 - a. Crie consultas para extrair padrões, visualizar dados de log e obter insights acionáveis.
3. Utilize o Contributor Insights Use o [CloudWatch Contributor Insights](#) para identificar os principais locutores em dimensões de alta cardinalidade, como endereços IP ou agentes-usuários.

4. Implemente filtros de métrica do CloudWatch Logs: configure [os filtros de métrica de log do CloudWatch](#) para converter dados de log em métricas acionáveis. Isso permite que você defina alarmes ou analise melhor os padrões.
5. Revisão e refinamento regulares: Revise periodicamente suas estratégias de análise de log para capturar todas as informações relevantes e otimizar continuamente o desempenho da aplicação.

Nível de esforço do plano de implementação: Médio.

Recursos

Práticas recomendadas relacionadas:

- [OPS04-BP01 Identificar os indicadores-chave de performance](#)
- [OPS04-BP02 Implementar a telemetria de aplicações](#)
- [OPS08-BP01 Analisar métricas de workload](#)

Documentos relacionados:

- [Análise de dados de log com o CloudWatch Logs Insights](#)
- [Uso do CloudWatch Contributor Insights](#)
- [Criação e gerenciamento de filtros de métrica de log do CloudWatch Logs](#)

Vídeos relacionados:

- [Analyze Log Data with CloudWatch Logs Insights \(Análise de dados de log com o CloudWatch Logs Insights\)](#)
- [Use CloudWatch Contributor Insights to Analyze High-Cardinality Data \(Use o CloudWatch Contributor Insights para analisar dados de alta cardinalidade\)](#)

Exemplos relacionados:

- [Exemplos de consultas do CloudWatch Logs](#)
- [Um workshop de observabilidade](#)

OPS08-BP03 Analisar rastreamentos de workload

Analisar dados de rastreamento é crucial para obter uma visão abrangente da jornada operacional de uma aplicação. Ao visualizar e compreender as interações entre vários componentes, o desempenho pode ser ajustado, os gargalos identificados e as experiências do usuário aprimoradas.

Resultado desejado: Obtenha uma visibilidade clara das operações distribuídas da sua aplicação, permitindo uma resolução mais rápida de problemas e uma experiência de usuário aprimorada.

Antipadrões comuns:

- Ignorar dados de rastreamento, confiando apenas em logs e métricas.
- Não correlacionar dados de rastreamento com logs associados.
- Ignorar as métricas derivadas de rastreamentos, como latência e taxas de falhas.

Benefícios de estabelecer esta prática recomendada:

- Aprimoramento da solução de problemas e redução do tempo médio de resolução (MTTR).
- Insights sobre dependências e seu impacto.
- Identificação e correção rápidas de problemas de desempenho.
- Uso de métricas derivadas de rastreamento para uma tomada de decisão informada.
- Experiências de usuário aprimoradas por meio de interações otimizadas de componentes.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

[O AWS X-Ray](#) oferece um pacote abrangente para análise de dados de rastreamento, fornecendo uma visão holística das interações de serviços, monitorando as atividades do usuário e detectando problemas de desempenho. Recursos como ServiceLens, X-Ray Insights, X-Ray Analytics e Amazon DevOps Guru aprimoram a profundidade dos insights acionáveis derivados de dados de rastreamento.

Etapas da implementação

As etapas a seguir oferecem uma abordagem estruturada para implementar com eficácia a análise de dados de rastreamento usando serviços da AWS:

1. Integre o AWS X-Ray: Integre o X-Ray às suas aplicações para capturar dados de rastreamento.
2. Analise métricas do X-Ray: Aprofunde-se em métricas derivadas de rastreamentos do X-Ray, como latência, taxas de solicitação, taxas de falhas e distribuições de tempo de resposta usando o [mapa de serviços](#) para monitorar a integridade da aplicação.
3. Use o ServiceLens: Use o [mapa do ServiceLens](#) para melhorar a observabilidade de seus serviços e aplicações. Isso permite a visualização integrada de rastreamentos, métricas, logs, alarmes e outras informações de integridade.
4. Habilite o X-Ray Insights:
 - a. Ative o [X-Ray Insights](#) para detecção automática de anomalias em rastreamentos.
 - b. Examine os insights para identificar padrões e determinar as causas principais, como maiores taxas de falhas ou latências.
 - c. Consulte o cronograma de insights para uma análise cronológica dos problemas detectados.
5. Use o X-Ray Analytics: [O X-Ray Analytics](#) permite que você explore minuciosamente os dados de rastreamento, identifique padrões e extraia insights.
6. Use grupos no X-Ray: Crie grupos no X-Ray para filtrar rastreamentos com base em critérios como alta latência, permitindo uma análise mais direcionada.
7. Incorpore o Amazon DevOps Guru: Use o [Amazon DevOps Guru](#) para se beneficiar dos modelos de machine learning que identificam anomalias operacionais nos rastreamentos.
8. Use o CloudWatch Synthetics: Use o [CloudWatch Synthetics](#) para criar canários para monitorar continuamente os endpoints e fluxos de trabalho. Esses canários podem integrar-se com o X-Ray para fornecer dados de rastreamento para uma análise aprofundada das aplicações que estão sendo testadas.
9. Use o Monitoramento de Usuários Reais (RUM): Com o [AWS X-Ray e o CloudWatch RUM](#), você pode analisar e depurar o caminho da solicitação a partir dos usuários finais de sua aplicação por meio de serviços downstream gerenciados pela AWS . Isso ajuda você a identificar tendências e erros de latência que afetam seus usuários.
10. Correlacionar com logs: Correlacione [dados de rastreamento com logs relacionados](#) dentro da visualização de rastreamento do X-Ray para uma perspectiva granular sobre o comportamento da aplicação. Isso permite que você visualize eventos de log diretamente associados às transações rastreadas.

Nível de esforço do plano de implementação: Médio.

Recursos

Práticas recomendadas relacionadas:

- [OPS08-BP01 Analisar métricas de workload](#)
- [OPS08-BP02 Analisar logs de workloads](#)

Documentos relacionados:

- [Uso do ServiceLens para monitorar a integridade da aplicação](#)
- [Explorar dados de rastreamento com o X-Ray Analytics](#)
- [Detectar anomalias em rastreamentos com o X-Ray Insights](#)
- [Monitorar continuamente com o CloudWatch Synthetics](#)

Vídeos relacionados:

- [Analyze and Debug Applications Using Amazon CloudWatch Synthetics and AWS X-Ray \(Analisar e depurar aplicações usando Amazon CloudWatch Synthetics e AWS X-Ray\)](#)
- [Use AWS X-Ray Insights \(Use o AWS X-Ray Insights\)](#)

Exemplos relacionados:

- [Um workshop de observabilidade](#)
- [Como implementar o X-Ray com o AWS Lambda](#)
- [Modelos canário do CloudWatch Synthetics](#)

OPS08-BP04 Criar alertas acionáveis

Detectar e responder prontamente aos desvios no comportamento da sua aplicação é crucial. É essencial reconhecer quando os resultados com base nos indicadores-chave de performance (KPIs) estão em risco ou quando surgem anomalias inesperadas. Basear alertas em KPIs garante que os sinais que você recebe estejam diretamente vinculados ao impacto comercial ou operacional. Essa abordagem de alertas acionáveis promove respostas proativas e ajuda a manter o desempenho e a confiabilidade do sistema.

Resultado desejado: Receba alertas oportunos, relevantes e acionáveis para rápida identificação e mitigação de possíveis problemas, especialmente quando os resultados do KPI estão em risco.

Antipadrões comuns:

- A configuração de muitos alertas não críticos leva à fadiga de alertas.
- A não priorização de alertas com base em KPIs dificulta a compreensão do impacto comercial dos problemas.
- A não abordagem das causas-raiz leva a alertas repetitivos para o mesmo problema.

Benefícios de estabelecer esta prática recomendada:

- Redução da fadiga de alertas ao se concentrar em alertas acionáveis e relevantes.
- Maior disponibilidade e confiabilidade do sistema por meio da detecção e mitigação proativas de problemas.
- Colaboração em equipe aprimorada e resolução mais rápida de problemas por meio da integração com ferramentas populares de alerta e comunicação.

Nível de risco exposto se esta prática recomendada não for estabelecida: alto

Orientação para implementação

Para criar um mecanismo de alerta eficaz, é fundamental usar métricas, logs e dados de rastreamento que sinalizem quando os resultados com base nos KPIs estão em risco ou quando anomalias são detectadas.

Etapas da implementação

1. Determine indicadores-chave de performance (KPIs): Identifique os KPIs de sua aplicação. Os alertas devem estar vinculados a esses KPIs para refletir com precisão o impacto nos negócios.
2. Implemente a detecção de anomalias:
 - Use o AWS Cost Anomaly Detection: configure o [AWS Cost Anomaly Detection](#) para detectar automaticamente padrões incomuns, garantindo que os alertas sejam gerados somente para anomalias genuínas.
 - Use o X-Ray Insights:
 - a. Configure o [X-Ray Insights](#) para detectar anomalias nos dados de rastreamento.
 - b. Configure [notificações no X-Ray Insights](#) para ser alertado sobre problemas detectados.

- Integre com o DevOps Guru:
 - a. Utilize o [Amazon DevOps Guru](#) devido a seus recursos de machine learning na detecção de anomalias operacionais com dados existentes.
 - b. Navegue até as [configurações de notificação](#) no DevOps Guru para configurar alertas de anomalias.
- 3. Implemente alertas acionáveis: Crie alertas que forneçam informações adequadas para ação imediata.
- 4. Reduza a fadiga de alarmes: Minimize os alertas não críticos. Equipes sobrecarregadas com vários alertas insignificantes podem não perceber problemas críticos e a eficácia geral do mecanismo de alerta fica diminuída.
- 5. Configurar alarmes compostos: Use os [alarmes compostos do Amazon CloudWatch](#) para consolidar vários alarmes.
- 6. Integre com ferramentas de alerta: Incorpore ferramentas como [Ops Genie](#) e [PagerDuty](#).
- 7. Utilize o AWS Chatbot integre o [AWS Chatbot](#) para retransmitir alertas para Chime, Microsoft Teams e Slack.
- 8. Alerta baseado em logs: Use o [filtros de métrica de log](#) no CloudWatch para criar alarmes com base em eventos de log específicos.
- 9. Revise e repita: Revise e revise regularmente as configurações de alerta.

Nível de esforço do plano de implementação: Médio.

Recursos

Práticas recomendadas relacionadas:

- [OPS04-BP01 Identificar os indicadores-chave de performance](#)
- [OPS04-BP02 Implementar a telemetria de aplicações](#)
- [OPS04-BP03 Implementar a telemetria da experiência do usuário](#)
- [OPS04-BP04 Implementar a telemetria de dependências](#)
- [OPS04-BP05 Implementar rastreamento distribuído](#)
- [OPS08-BP01 Analisar métricas de workload](#)
- [OPS08-BP02 Analisar logs de workloads](#)
- [OPS08-BP03 Analisar rastreamentos de workload](#)

Documentos relacionados:

- [Uso dos alarmes do Amazon CloudWatch](#)
- [Crie um alarme composto](#)
- [Crie um alarme do CloudWatch com base na detecção de anomalias](#)
- [Notificações do DevOps Guru](#)
- [Notificações do X-Ray Insights](#)
- [Monitore, opere e solucione problemas de seus recursos da AWS com ChatOps interativos](#)
- [Guia de integração do Amazon CloudWatch | PagerDuty](#)
- [Integre o OpsGenie com o Amazon CloudWatch](#)

Vídeos relacionados:

- [Create Composite Alarms in Amazon CloudWatch \(Criar alarmes compostos no Amazon CloudWatch\)](#)
- [AWS Chatbot Overview \(Visão geral do AWS Chatbot\)](#)
- [AWS on Air ft. Mutative Commands in AWS Chatbot \(Comandos mutativos no AWS Chatbot\)](#)

Exemplos relacionados:

- [Alarmes, gerenciamento de incidentes e remediação na nuvem com o Amazon CloudWatch](#)
- [Tutorial: criação de uma regra do Amazon EventBridge que envia notificações para o AWS Chatbot](#)
- [Um workshop de observabilidade](#)

OPS08-BP05 Criar painéis

Os painéis são a visão centrada no ser humano dos dados de telemetria de suas workloads. Embora forneçam uma interface visual vital, eles não devem substituir os mecanismos de alerta, mas sim complementá-los. Quando elaborados com cuidado, eles não apenas oferecem insights rápidos sobre a integridade e o desempenho do sistema, como também podem apresentar às partes interessadas informações em tempo real sobre os resultados empresariais e o impacto dos problemas.

Resultado desejado: Insights claros e acionáveis sobre a integridade do sistema e dos negócios usando representações visuais.

Antipadrões comuns:

- Painéis complicados demais e com muitas métricas.
- Confiar em painéis sem alertas para detecção de anomalias.
- Não atualizar os painéis à medida que as workloads evoluem.

Benefícios de estabelecer esta prática recomendada:

- Visibilidade imediata das métricas e KPIs críticos do sistema.
- Comunicação e compreensão aprimoradas com as partes interessadas.
- Visão rápida do impacto dos problemas operacionais.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Painéis centrados nos negócios

Painéis personalizados para os KPIs de negócios envolvem uma gama maior de partes interessadas. Embora essas pessoas possam não estar interessadas nas métricas do sistema, elas estão interessadas em entender as implicações comerciais desses números. Um painel centrado nos negócios garante que todas as métricas técnicas e operacionais monitoradas e analisadas estejam sincronizadas com as metas empresariais abrangentes. Esse alinhamento fornece clareza, garantindo que todos estejam em sintonia sobre o que é essencial e o que não é. Além disso, painéis que destacam os KPIs de negócios tendem a ser mais acionáveis. As partes interessadas podem entender rapidamente a integridade das operações, as áreas que precisam de atenção e o impacto potencial nos resultados empresariais.

Com isso em mente, ao criar seus painéis, garanta que haja um equilíbrio entre métricas técnicas e KPIs comerciais. Ambos são vitais, mas atendem a públicos diferentes. O ideal é que você tenha painéis que forneçam uma visão holística da integridade e do desempenho do sistema e, ao mesmo tempo, enfatizem os principais resultados comerciais e suas implicações.

Os painéis do Amazon CloudWatch são páginas iniciais personalizáveis no console do CloudWatch, que você pode usar para monitorar os recursos em uma única visualização, mesmo aqueles distribuídos por Regiões da AWS e contas diferentes.

Etapas da implementação

1. Crie um painel básico: [crie um novo painel no CloudWatch](#) dê a ele um nome descritivo.
2. Use widgets de Markdown: antes de mergulhar nas métricas, use [widgets de Markdown](#) para adicionar contexto textual na parte superior do painel. Isso deve explicar o que o painel abrange, a importância das métricas representadas e também pode conter links para outros painéis e ferramentas de solução de problemas.
3. Crie variáveis do painel: [incorpore variáveis do painel](#) quando apropriado, para permitir visualizações dinâmicas e flexíveis do painel.
4. Crie widgets de métricas: [adicione widgets de métricas](#) para visualizar várias métricas que sua aplicação emite, adaptando esses widgets para representar com eficácia a integridade do sistema e os resultados empresariais.
5. Consultas do Log Insights: utilize o [CloudWatch Logs Insights](#) para obter métricas acionáveis de seus logs e exibir esses insights em seu painel.
6. Configurar alarmes: integre [alarmes do CloudWatch](#) em seu painel para uma visão rápida de qualquer métrica que esteja ultrapassando seus limites.
7. Use o Contributor Insights: incorpore o [CloudWatch Contributor Insights](#) para analisar campos de alta cardinalidade e obter uma compreensão mais clara dos principais colaboradores do seu recurso.
8. Crie widgets personalizados: para necessidades específicas não atendidas pelos widgets padrão, considere criar [widgets personalizados](#). Eles podem ser extraídos de várias fontes de dados ou representar dados de maneiras exclusivas.
9. Repita e refine: à medida que sua aplicação evolui, revise regularmente seu painel para garantir sua relevância.

Recursos

Práticas recomendadas relacionadas:

- [OPS04-BP01 Identificar os indicadores-chave de performance](#)
- [OPS08-BP01 Analisar métricas de workload](#)
- [OPS08-BP02 Analisar logs de workloads](#)
- [OPS08-BP03 Analisar rastreamentos de workload](#)
- [OPS08-BP04 Criar alertas acionáveis](#)

Documentos relacionados:

- [Criação de painéis para visibilidade operacional](#)
- [Uso de painéis do Amazon CloudWatch](#)

Vídeos relacionados:

- [Create Cross Account & Cross Region CloudWatch Dashboards \(Criar painéis do CloudWatch entre contas e entre regiões\)](#)
- [AWS re:Invent 2021 - Gain enterprise visibility with Nuvem AWS operation dashboards \(AWS re:Invent 2021: obtenha visibilidade corporativa com painéis de operação do CloudWatch\)](#)

Exemplos relacionados:

- [Um workshop de observabilidade](#)
- [Monitoramento de aplicações do Amazon CloudWatch](#)

Compreensão da integridade operacional

Defina, capture e analise as métricas de operações para obter visibilidade das atividades de equipes de operações e tomar ações apropriadas.

Sua organização deve entender facilmente a integridade operacional de suas operações. Defina as metas de negócios das equipes de operações, identifique os indicadores-chave de performance que as refletem e use e desenvolva métricas com base nos resultados operacionais para obter informações úteis. Use essas métricas para implementar painéis e relatórios com pontos de vista técnicos e de negócios que ajudarão os líderes e as partes interessadas a tomar decisões informadas.

A AWS facilita a reunião e a análise de logs de operações para que você possa gerar métricas, conhecer o status de suas operações e obter insights sobre as operações ao longo do tempo.

Práticas recomendadas

- [OPS09-BP01 Medir metas operacionais e KPIs com métricas](#)
- [OPS09-BP02 Comunicar o status e as tendências para garantir a visibilidade da operação](#)
- [OPS09-BP03 Revisar as métricas operacionais e priorizar a melhoria](#)

OPS09-BP01 Medir metas operacionais e KPIs com métricas

Obtenha metas e KPIs que definam o sucesso das operações de sua organização e determine se as métricas os refletem. Defina linhas de base como ponto de referência e reavalie regularmente. Desenvolva mecanismos para coletar essas métricas das equipes para avaliação.

Resultado desejado:

- As metas e os KPIs das equipes de operações da organização foram publicados e compartilhados.
- Métricas que refletem esses KPIs são estabelecidas. Os exemplos podem incluir:
 - Profundidade da fila de tíquetes ou idade média do tíquete
 - Contagem de tíquetes agrupada por tipo de problema
 - Tempo gasto trabalhando em problemas com ou sem um procedimento operacional padronizado (SOP)
 - Tempo gasto na recuperação de uma falha no envio de código
 - Volume de chamadas

Antipadrões comuns:

- Os prazos de implantação são perdidos porque os desenvolvedores são contratados para realizar tarefas de solução de problemas. As equipes de desenvolvimento demandam mais pessoal, mas não conseguem quantificar quantos precisam porque o tempo perdido não pode ser medido.
- Um atendimento de Nível 1 foi configurado para lidar com chamadas de usuários. Com o tempo, mais workloads foram adicionadas, mas nenhum número de funcionários foi alocado para o atendimento de Nível 1. A satisfação do cliente sofre à medida que os tempos de atendimento aumentam e os problemas ficam mais tempo sem resolução, mas a gerência não vê indicadores disso, impedindo qualquer ação.
- Uma workload problemática foi transferida para uma equipe de operações separada para manutenção. Diferentemente de outras workloads, a nova não foi fornecida com documentação e runbooks adequados. Dessa forma, as equipes passam mais tempo solucionando problemas e tratando de falhas. No entanto, não há métricas que documentem isso, o que dificulta a prestação de contas.

Benefícios de estabelecer esta prática recomendada: Onde o monitoramento da workload mostra o estado de nossas aplicações e serviços, as equipes de operações de monitoramento fornecem

aos proprietários uma visão das mudanças entre os consumidores dessas workloads, como as mudanças nas necessidades dos negócios. Meça a eficácia dessas equipes e avalie-as em relação às metas de negócios, criando métricas que possam refletir o estado das operações. As métricas podem destacar problemas de suporte ou identificar quando ocorrem desvios de uma meta de nível de serviço.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Agende um horário com líderes de negócios e partes interessadas para determinar as metas gerais do serviço. Determine quais devem ser as tarefas de várias equipes de operações e quais desafios elas podem enfrentar. Com isso, pense em indicadores-chave de performance (KPIs) que possam refletir essas metas operacionais. Pode ser a satisfação do cliente, o tempo desde a concepção do recurso até a implantação, o tempo médio de resolução de problemas e outros.

Trabalhando a partir de KPIs, identifique as métricas e as fontes de dados que podem refletir melhor essas metas. A satisfação do cliente pode ser uma combinação de várias métricas, como tempos de espera ou resposta de chamadas, índices de satisfação e tipos de problemas levantados. Os tempos de implantação podem ser a soma do tempo necessário para testes e implantação e quaisquer correções pós-implantação que precisem ser adicionadas. As estatísticas que mostram o tempo gasto em diferentes tipos de problemas (ou a contagem desses problemas) podem fornecer uma visão de onde é necessário um esforço direcionado.

Recursos

Documentos relacionados:

- [Amazon QuickSight: uso de KPIs](#)
- [Amazon CloudWatch: uso de métricas](#)
- [Criação de painéis](#)
- [Como rastrear seus KPIs de otimização de custos com o painel de KPI](#)

OPS09-BP02 Comunicar o status e as tendências para garantir a visibilidade da operação

É necessário conhecer o estado de suas operações e a direção das tendências para identificar quando os resultados podem estar em risco, se o trabalho adicional pode ou não ser apoiado ou os

efeitos que as mudanças tiveram em suas equipes. Durante eventos operacionais, ter páginas de status que os usuários e as equipes operacionais possam consultar para obter informações pode reduzir a pressão nos canais de comunicação e disseminar informações de forma proativa.

Resultado desejado:

- Os líderes de operações têm uma visão rápida para ver em que tipo de volume de chamadas suas equipes estão operando e quais esforços podem estar em andamento, como implantações.
- Os alertas são disseminados para as partes interessadas e comunidades de usuários quando ocorrem impactos nas operações normais.
- A liderança da organização e as partes interessadas podem verificar uma página de status em resposta a um alerta ou impacto e obter informações sobre um evento operacional, como pontos de contato, informações sobre tíquetes e tempos estimados de recuperação.
- Os relatórios são disponibilizados para a liderança e outras partes interessadas para mostrar estatísticas operacionais, como volumes de chamadas durante um período de tempo, índices de satisfação do usuário, números de tíquetes pendentes e suas idades.

Antipadrões comuns:

- Uma workload diminui, deixando um serviço indisponível. O volume de chamadas aumenta à medida que os usuários solicitam saber o que está acontecendo. Os gerentes aumentam o volume de solicitações para saber quem está resolvendo um problema. Várias equipes de operações duplicam esforços na tentativa de investigar.
- O desejo por uma nova capacidade faz com que vários funcionários sejam transferidos para um esforço de engenharia. Nenhum preenchimento é fornecido e os tempos de resolução de problemas aumentam. Essas informações não são capturadas e a liderança toma conhecimento do problema somente após várias semanas de comentários de insatisfação do usuário.

Benefícios de estabelecer esta prática recomendada: durante eventos operacionais em que a empresa é afetada, muito tempo e energia podem ser desperdiçados consultando informações de várias equipes tentando entender a situação. Ao estabelecer páginas de status e painéis amplamente divulgados, as partes interessadas podem obter rapidamente informações, como se um problema foi detectado ou não, quem liderou o problema ou quando é esperado um retorno às operações normais. Isso permite que os membros da equipe dediquem mais tempo à resolução de problemas e passem menos tempo comunicando o status a outras pessoas.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Crie painéis que mostrem as principais métricas atuais para suas equipes de operações e torne-as facilmente acessíveis, tanto para os líderes de operações quanto para a gerência.

Crie páginas de status que possam ser atualizadas rapidamente para mostrar quando um incidente ou evento está ocorrendo, quem é o proprietário e quem está coordenando a resposta. Compartilhe todas as etapas ou soluções alternativas que os usuários devem considerar nesta página e divulgue amplamente a localização. Incentive os usuários a verificar esse local primeiro quando confrontados com um problema desconhecido.

Colete e forneça relatórios que mostrem a integridade das operações ao longo do tempo e distribua-os aos líderes e tomadores de decisão para ilustrar o trabalho das operações junto com os desafios e as necessidades.

Compartilhe entre as equipes essas métricas e relatórios que melhor refletem as metas e os KPIs e onde eles foram influentes na promoção da mudança. Dedique tempo a essas atividades para aumentar a importância das operações dentro das equipes e entre elas.

Recursos

Documentos relacionados:

- [Avalie o progresso](#)
- [Criação de painéis para visibilidade da operação](#)

Soluções relacionadas:

- [Operações de dados](#)

OPS09-BP03 Revisar as métricas operacionais e priorizar a melhoria

Reservar tempo e dedicar recursos para analisar o estado das operações garante que atender à linha de negócios do dia a dia continue sendo uma prioridade. Reúna líderes de operações e partes interessadas para revisar regularmente as métricas, reafirmar ou modificar metas e objetivos e priorizar melhorias.

Resultado desejado:

- Os líderes de operações e a equipe se reúnem regularmente para revisar as métricas durante um determinado período do relatório. Os desafios são comunicados, as vitórias são celebradas e as lições aprendidas são compartilhadas.
- As partes interessadas e os líderes de negócios são regularmente informados sobre o estado das operações e solicitados a fornecer informações sobre metas, KPIs e iniciativas futuras. As compensações entre prestação de serviços, operações e manutenção são discutidas e contextualizadas.

Antipadrões comuns:

- Um novo produto é lançado, mas as equipes operacionais de nível 1 e nível 2 não são adequadamente treinadas para dar suporte nem recebem pessoal adicional. Métricas que mostram a diminuição nos tempos de resolução de tíquetes e o aumento nos volumes de incidentes não são vistas pelos líderes. Uma ação é tomada semanas depois, quando os números de assinaturas começam a cair à medida que usuários insatisfeitos saem da plataforma.
- Um processo manual para realizar a manutenção de uma workload está em vigor há muito tempo. Embora o desejo de automatizar estivesse presente, essa era uma prioridade baixa, dada a baixa importância do sistema. No entanto, com o tempo, o sistema cresceu em importância e agora esses processos manuais consomem a maior parte do tempo das operações. Nenhum recurso está programado para fornecer mais ferramentas às operações, causando o esgotamento da equipe à medida que as workloads aumentam. A liderança percebe o que está acontecendo quando é relatado que funcionários estão indo trabalhar para outros concorrentes.

Benefícios de estabelecer esta prática recomendada: em algumas organizações, pode ser um desafio alocar o mesmo tempo e atenção dedicados à prestação de serviços e a novos produtos ou ofertas. Quando isso ocorre, a linha de negócios pode sofrer enquanto o nível de serviço esperado se deteriora lentamente. Isso ocorre porque as operações não mudam e evoluem com o crescimento dos negócios e logo podem ser deixadas para trás. Sem uma análise regular dos insights que as operações coletam, o risco para a empresa pode se tornar visível somente quando for tarde demais. Ao alocar tempo para revisar métricas e procedimentos tanto entre a equipe de operações quanto com a liderança, o papel crucial que as operações desempenham permanece visível e os riscos podem ser identificados muito antes de atingirem níveis críticos. As equipes de operações obtêm uma visão melhor das mudanças e iniciativas comerciais iminentes, permitindo que esforços proativos sejam realizados. A visibilidade da liderança nas métricas operacionais mostra o papel que essas equipes desempenham na satisfação do cliente, tanto interna quanto externa, e permite

que elas avaliem melhor as opções de prioridades ou garantam que as operações tenham tempo e recursos para mudar e evoluir com novas iniciativas de negócios e workload.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Dedique tempo para analisar as métricas operacionais entre as partes interessadas e as equipes operacionais e analisar os dados do relatório. Coloque esses relatórios nos contextos das metas e objetivos da organização para determinar se eles estão sendo cumpridos. Identifique fontes de ambiguidade onde as metas não são claras ou onde pode haver conflitos entre o que é pedido e o que é dado.

Identifique onde o tempo, as pessoas e as ferramentas podem ajudar nos resultados das operações. Determine quais KPIs isso afetaria e quais deveriam ser as metas de sucesso. Revise regularmente para garantir que as operações tenham recursos suficientes para apoiar a linha de negócios.

Recursos

Documentos relacionados:

- [Amazon Athena](#)
- [Amazon CloudWatch metrics and dimensions reference \(Métricas do Amazon CloudWatch e referência de dimensões\)](#)
- [Amazon QuickSight](#)
- [AWS Glue](#)
- [AWS Glue Data Catalog](#)
- [Collect metrics and logs from Amazon EC2 instances and on-premises servers with the Amazon CloudWatch Agent \(Coletar métricas e logs das instâncias do Amazon EC2 e de servidores on-premises com o agente do Amazon CloudWatch\)](#)
- [Using Amazon CloudWatch metrics \(Uso de métricas do Amazon CloudWatch\)](#)

Resposta a eventos

Antecipe eventos operacionais, planejados (por exemplo, promoções de vendas, implantações e testes de falha) e não planejados (por exemplo, picos de utilização e falhas de componentes).

Use seus runbooks e playbooks existentes para fornecer resultados consistentes ao responder a alertas. Os alertas definidos devem pertencer a uma função ou equipe responsável pela resposta e escalacões. Você também deseja conhecer o impacto comercial dos componentes do sistema e usá-lo para direcionar esforços quando necessário. Execute uma análise de causa-raiz (RCA) após os eventos e impeça a recorrência de falhas ou soluções alternativas de documentos.

A AWS simplifica a resposta a eventos fornecendo ferramentas compatíveis com todos os aspectos da workload e das operações como código. Essas ferramentas permitem criar scripts de respostas a eventos de operações e acionar sua execução em resposta aos dados de monitoramento.

Na AWS, é possível melhorar o tempo de recuperação substituindo componentes com falha por novas versões íntegras, em vez de tentar repará-los. Em seguida, você pode executar a análise do recurso com falha fora de banda.

Práticas recomendadas

- [OPS10-BP01 Usar um processo para gerenciamento de eventos, incidentes e problemas](#)
- [OPS10-BP02 Ter um processo por alerta](#)
- [OPS10-BP03 Priorizar eventos operacionais com base no impacto nos negócios](#)
- [OPS10-BP04 Definir caminhos para escaladas](#)
- [OPS10-BP05 Definir um plano de comunicação com o cliente para interrupções](#)
- [OPS10-BP06 Comunicar o status por meio de painéis](#)
- [OPS10-BP07 Automatizar respostas a eventos](#)

OPS10-BP01 Usar um processo para gerenciamento de eventos, incidentes e problemas

Sua organização tem processos para lidar com eventos, incidentes e problemas. Eventos são coisas que ocorrem em sua workload que talvez não precisem de intervenção. Incidentes são eventos que requerem intervenção. Problemas são eventos recorrentes que exigem intervenção ou que não podem ser resolvidos. São necessários processos para reduzir o impacto desses eventos sobre os negócios e garantir respostas adequadas.

Quando incidentes e problemas acontecem em sua workload, você precisa de processos para lidar com eles. Como você vai comunicar o status do evento às partes interessadas? Quem supervisiona e lidera a resposta? Quais são as ferramentas usadas para mitigar o evento? Esses são alguns exemplos de perguntas que você precisa responder para ter um processo de resposta sólido.

Os processos devem estar documentados em um local central e disponíveis a todos envolvidos com a workload. Se você não tiver uma wiki ou um armazenamento central de documentos, use um repositório de controle de versão. Você vai manter esses planos atualizados à medida que os processos evoluem.

Problemas são candidatos para automação. Esses eventos consomem o tempo que você poderia usar para inovar. Comece criando um processo repetível para mitigar o problema. Com o tempo, concentre-se na automação da mitigação ou correção do problema subjacente. Isso vai liberar tempo que você poderá dedicar ao desenvolvimento de melhorias para a workload.

Resultado desejado: sua organização tem processos para lidar com eventos, incidentes e problemas. Esses processos são documentados e armazenados em um local central. Eles são atualizados à medida que os processos mudam.

Antipadrões comuns:

- Um acidente ocorre durante um final de semana e o engenheiro de plantão não sabe o que fazer.
- Um cliente envia um e-mail informando que a aplicação está fora do ar. Você reinicializa o servidor para corrigir. Isso acontece com frequência.
- Há um incidente com várias equipes trabalhando de maneira independente para resolvê-lo.
- As implantações acontecem na workload sem serem registradas.

Benefícios do estabelecimento desta prática recomendada:

- Você tem uma trilha de auditoria de eventos na workload.
- O tempo para se recuperar de um incidente diminui.
- Os membros da equipe podem resolver incidentes e problemas de maneira consistente.
- Há um esforço mais consolidado na hora de investigar um incidente.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação de implementação

Implementar essa prática recomendada significa que você está monitorando os eventos da workload. Você tem processos para lidar com incidentes e problemas. Os processos são documentados, compartilhados e atualizados com frequência. Problemas são identificados, priorizados e corrigidos.

Exemplo de cliente

A AnyCompany Retail tem uma parte de sua wiki interna dedicada a processos para gerenciamento de eventos, incidentes e problemas. Todos os eventos são enviados para o [Amazon EventBridge](#). Os problemas são identificados como OpsItems no [OpsCenter do AWS Systems Manager](#) e priorizados para correção, reduzindo a mão de obra não diferenciada. À medida que os processos mudam, eles são atualizados na wiki interna. Eles usam o [AWS Systems Manager Incident Manager](#) para gerenciar incidentes e coordenar os esforços de mitigação.

Etapas da implementação

1. Eventos

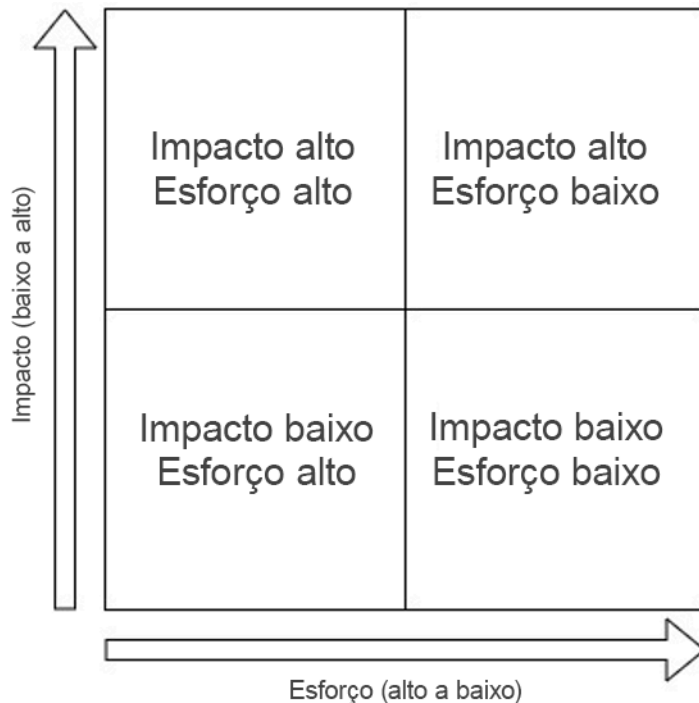
- Monitore os eventos que acontecem na workload, mesmo que nenhuma intervenção humana seja necessária.
- Trabalhe com as partes interessadas da workload para desenvolver uma lista de eventos que devem ser monitorados. Alguns exemplos são implantações concluídas ou aplicações de correções bem-sucedidas.
- Você pode usar serviços como [Amazon EventBridge](#) ou [Amazon Simple Notification Service](#) para gerar eventos personalizados para monitoramento.

2. Incidentes

- Comece definindo o plano de comunicação para incidentes. Quais partes interessadas devem ser informadas? Como você vai mantê-las informadas? Quem supervisiona os esforços de coordenação? Recomendamos a configuração de um canal de bate-papo interno para comunicação e coordenação.
- Defina caminhos de encaminhamento para as equipes que oferecem suporte à workload, principalmente se a equipe não tiver uma rotação de plantão. Com base em seu nível de suporte, você também pode registrar um caso no AWS Support.
- Crie um playbook para investigar o incidente. Isso deve incluir o plano de comunicação e etapas de investigação detalhadas. Inclua a verificação do [AWS Health Dashboard](#) na investigação.
- Documente seu plano de resposta a incidentes. Comunique o plano de gerenciamento de incidentes para que clientes internos e externos entendam as regras de engajamento e o que espera-se deles. Treine os membros de sua equipe sobre como usá-lo.
- Os clientes podem usar o [Incident Manager](#) para configurar e gerenciar seu respectivo plano de resposta a incidentes.
- Os clientes Enterprise Support podem solicitar o [Workshop de gerenciamento de incidentes](#) de seu gerente de conta técnico. Esse workshop guiado testa seu plano de resposta a incidentes e ajuda você a identificar áreas para melhoria.

3. Problemas

- Os problemas devem ser identificados e monitorados em seu sistema de ITSM.
- Identifique todos os problemas conhecidos e priorize-os em termos de esforço para corrigir e impacto na workload.



- Resolva problemas de alto impacto e pouco esforço primeiro. Com esses resolvidos, passe para os problemas do quadrante de baixo impacto e pouco esforço.
- Você pode usar o [OpsCenter do Systems Manager](#) para identificar esses problemas, anexar runbooks a eles e monitorá-los.

Nível de esforço do plano de implementação: médio. Você precisa de um processo e ferramentas para implementar essa prática recomendada. Documente seus processos e disponibilize-os para todos que estão associados à workload. Atualize-os com frequência. Você tem um processo para gerenciar problemas e mitigá-los ou corrigi-los.

Recursos

Práticas recomendadas relacionadas:

- [OPS07-BP03 Usar runbooks para realizar procedimentos](#): problemas conhecidos precisam de um runbook associado para que os esforços de mitigação sejam consistentes.

- [OPS07-BP04 Usar manuais para investigar problemas](#): os incidentes precisam ser investigados usando playbooks.
- [OPS11-BP02 Executar análise pós-incidente](#): sempre conduza uma autópsia depois de se recuperar de um incidente.

Documentos relacionados:

- [Atlassian: gerenciamento de incidentes na era de DevOps](#)
- [Guia de resposta a incidentes de segurança da AWS](#)
- [Gerenciamento de incidentes na era de DevOps e SRE](#)
- [PagerDuty: o que é gerenciamento de incidentes?](#)

Vídeos relacionados:

- [AWS re:Invent 2020: Incident management in a distributed organization \(AWS re:Invent 2020: gerenciamento de incidentes em uma organização distribuída\)](#)
- [AWS re:Invent 2021 - Building next-gen applications with event-driven architectures \(AWS re:Invent 2021 - criando aplicações de última geração com arquiteturas orientadas por eventos\)](#)
- [AWS Supports You | Exploring the Incident Management Tabletop Exercise \(AWS apoia você | Conhecendo a simulação teórica de gerenciamento de incidentes\)](#)
- [AWS Systems Manager Incident Manager - AWS Virtual Workshops \(AWS Systems Manager Incident Manager - workshops virtuais da AWS\)](#)
- [AWS What's Next ft. Incident Manager | AWS Events \(Próximos passos na AWS com Incident Manager | Eventos da AWS\)](#)

Exemplos relacionados:

- [workshop de ferramentas de gerenciamento e governança da AWS - OpsCenter](#)
- [Serviços proativos da AWS: workshop de gerenciamento de incidentes](#)
- [Como desenvolver uma aplicação orientada por eventos com o Amazon EventBridge](#)
- [Como desenvolver arquiteturas orientadas por eventos na AWS](#)

Serviços relacionados:

- [Amazon EventBridge](#)
- [Amazon SNS](#)
- [AWS Health Dashboard](#)
- [AWS Systems Manager Incident Manager](#)
- [OpsCenter do AWS Systems Manager](#)

OPS10-BP02 Ter um processo por alerta

Tenha uma resposta bem-definida (runbook ou playbook), com um proprietário especificamente identificado, para qualquer evento para o qual você acione um alerta. Isso garante respostas eficazes e rápidas aos eventos de operações e evita que eventos acionáveis sejam ocultados por notificações menos valiosas.

Antipadrões comuns:

- Seu sistema de monitoramento apresenta um stream de conexões aprovadas junto com outras mensagens. O volume de mensagens é tão grande que você perde mensagens de erro periódicas que exigem sua intervenção.
- Você recebe um alerta de que o site está inoperante. Não há um processo definido para quando isso acontece. Você é forçado a adotar uma abordagem ad hoc para diagnosticar e resolver o problema. Desenvolver esse processo conforme o uso estende o tempo para recuperação.

Benefícios do estabelecimento desta prática recomendada: Ao alertar somente quando uma ação é necessária, você impede que alertas de valor baixo ocultem alertas de valor alto. Ao ter um processo para alertas sempre acionáveis, você permite uma resposta consistente e imediata a eventos em seu ambiente.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Alto

Orientações para a implementação

- Processo por alerta: qualquer evento para o qual você dispara um alerta deve ter uma resposta bem-definida (runbook ou manual) com um proprietário identificado especificamente (por exemplo, indivíduo, equipe ou função) responsável pela execução bem-sucedida. O desempenho da resposta pode ser automatizado ou conduzido por outra equipe, mas o proprietário é responsável por garantir que o processo ofereça os resultados esperados. Ao ter esses processos, você

garante respostas eficazes e rápidas aos eventos de operações e pode impedir que eventos acionáveis sejam ocultados por notificações menos valiosas. Por exemplo, o auto scaling pode ser aplicado para dimensionar um front-end da web, mas a equipe de operações pode ser responsável por garantir que as regras e os limites de auto scaling sejam adequados para as necessidades de carga de trabalho.

Recursos

Documentos relacionados:

- [Recursos do Amazon CloudWatch](#)
- [O que é o Amazon CloudWatch Events?](#)

Vídeos relacionados:

- [Build a monitoring plan](#)

OPS10-BP03 Priorizar eventos operacionais com base no impacto nos negócios

Quando vários eventos demandarem intervenção, aborde primeiro os mais significativos para os negócios. Os impactos podem incluir perda de vida ou ferimentos, perda financeira ou danos à reputação ou confiança.

Antipadrões comuns:

- Você recebe uma solicitação de suporte para adicionar uma configuração de impressora para um usuário. Ao trabalhar no problema, você recebe uma solicitação de suporte informando que o site de varejo está inoperante. Depois de concluir a configuração da impressora para o usuário, você começa a trabalhar no problema do site.
- Você é notificado de que o site de varejo e o sistema de folha de pagamento estão inoperantes. Você não sabe para qual deve ter prioridade.

Benefícios do estabelecimento desta prática recomendada: A priorização de respostas aos incidentes com o maior impacto na empresa permite que você gerencie esse impacto.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

- Priorizar eventos operacionais com base no impacto empresarial: garanta que, quando vários eventos exigirem intervenção, aqueles que forem mais significativos para a empresa sejam abordados primeiro. Os impactos podem incluir perda de vida ou ferimentos, perda financeira, violações regulatórias ou danos à reputação ou à confiança.

OPS10-BP04 Definir caminhos para escaladas

Defina caminhos de escalação em seus runbooks e playbooks, incluindo o que aciona a escalação e os procedimentos para escalação. Identifique especificamente os proprietários de cada ação para garantir respostas eficazes e rápidas aos eventos de operações.

Saiba quando é necessária uma decisão humana antes que medidas sejam tomadas. Trabalhe com os tomadores de decisão para que essa decisão seja tomada antecipadamente e a ação seja pré-aprovada, para que a MTTR não seja estendida aguardando uma resposta.

Antipadrões comuns:

- Seu site de varejo está inoperante. Você não compreende o runbook para recuperar o site. Você começa a chamar colegas na expectativa de que alguém possa ajudá-lo.
- Você recebe um caso de suporte para um aplicativo inacessível. Você não tem permissões para administrar o sistema. Você não sabe quem tem. Você tenta entrar em contato com o proprietário do sistema que abriu o caso e não há resposta. Você não tem contatos do sistema e seus colegas não estão familiarizados com ele.

Benefícios do estabelecimento desta prática recomendada: Ao definir escalações, gatilhos para escalação e procedimentos para escalação, você permite a adição sistemática de recursos a um incidente a uma taxa apropriada para o impacto.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Médio

Orientações para a implementação

- Definir caminhos para as escaladas: defina caminhos para as escaladas em seus runbooks e manuais, incluindo que é acionado pela escalada e os respectivos procedimentos. Por exemplo, escalação de um problema de engenheiros de suporte para engenheiros de suporte seniores quando a resolução do problema não estiver nos runbooks ou quando um período de tempo

predefinido tiver decorrido. Outro exemplo de um caminho de escalação apropriado é dos engenheiros de suporte sênior à equipe de desenvolvimento para uma carga de trabalho quando os playbooks não conseguem identificar um caminho para a correção ou quando um período de tempo predefinido decorre. Identifique especificamente os proprietários de cada ação para garantir respostas eficazes e rápidas aos eventos de operações. Os escalonamentos podem incluir terceiros. Por exemplo, um provedor de conectividade de rede ou um fornecedor de software. Os escalonamentos podem incluir tomadores de decisão autorizados identificados para sistemas impactados.

OPS10-BP05 Definir um plano de comunicação com o cliente para interrupções

Defina e teste um plano de comunicação para interrupções do sistema que seja confiável para manter os clientes e as partes interessadas informados durante interrupções. Comunique-se diretamente com os usuários tanto quando os serviços que eles usam forem afetados como quando os serviços voltarem ao normal.

Resultado desejado:

- Você tem um plano de comunicação para situações que vão desde manutenção agendada até grandes falhas inesperadas, incluindo invocação de planos de recuperação de desastres.
- Nas comunicações, você fornece informações claras e transparentes sobre problemas do sistema para ajudar os clientes a evitar dúvidas sobre o desempenho dos sistemas.
- Você usa mensagens de erro personalizadas e páginas de status para reduzir o pico nas solicitações de suporte técnico e mantém os usuários informados.
- O plano de comunicação é testado regularmente para verificar se ele ocorrerá como planejado no caso de uma interrupção real.

Antipadrões comuns:

- Ocorre uma interrupção da workload, mas você não tem um plano de comunicação. Os usuários sobrecarregam o sistema de tíquetes com solicitações, pois não têm informações sobre a interrupção.
- Você envia uma notificação por e-mail aos usuários durante uma interrupção. Ela não contém um prazo para a restauração do serviço, então os usuários não conseguem se planejar em torno da interrupção.

- Há um plano de comunicação para interrupções, mas ele nunca foi testado. Ocorre uma interrupção e o plano de comunicação falha, pois faltou uma etapa fundamental que poderia ter sido identificada no teste.
- Durante uma interrupção, você envia uma notificação aos usuários com muitas informações e detalhes técnicos sob o NDA da AWS.

Benefícios do estabelecimento desta prática recomendada:

- Manter a comunicação durante as interrupções garante que os clientes possam ver o andamento da resolução dos problemas e o tempo previsto para que ela ocorra.
- Desenvolver um plano de comunicação bem-definido garante que os clientes e usuários finais estejam bem-informados para que possam tomar medidas adicionais visando a mitigar o impacto das interrupções.
- Com uma comunicação adequada e maior ciência acerca de interrupções planejadas e não planejadas, é possível melhorar a satisfação dos clientes, limitar reações não pretendidas e gerar a retenção dos clientes.
- Uma comunicação transparente e em tempo hábil acerca da interrupção do sistema gera credibilidade e estabelece a confiança necessária para manter seu relacionamento com os clientes.
- Uma estratégia de comunicação comprovada durante uma interrupção ou crise reduz a especulação e os rumores que poderiam atrapalhar sua capacidade de recuperação.

Nível de risco exposto se esta prática recomendada não é estabelecida: médio

Orientações para a implementação

Os planos de comunicação que mantêm os clientes informados durante interrupções são holísticos e abrangem várias interfaces, incluindo páginas de erro voltadas para o cliente, mensagens de erro de API personalizadas, banners sobre o status do sistema e páginas de status de integridade. Se o sistema incluir usuários registrados, é possível comunicar-se por canais de mensagens, como e-mail, SMS ou notificações por push, para enviar conteúdo com mensagens personalizadas aos clientes.

Ferramentas de comunicação com o cliente

Como uma primeira linha de defesa, as aplicações web e móveis devem fornecer mensagens de erro amistosas e informativas durante uma interrupção e devem poder redirecionar o tráfego para uma página de status. O [Amazon CloudFront](#) é uma rede de entrega de conteúdo (CDN) que inclui

recursos para definir e entregar conteúdo de erro personalizado. As páginas de erro personalizadas no CloudFront são uma ótima camada inicial de mensagens para os clientes para interrupções no nível de componentes. O CloudFront também pode simplificar o gerenciamento e a ativação da página de status para interceptar todas as solicitações durante interrupções planejadas e não planejadas.

As mensagens de erro de API personalizadas podem ajudar a detectar e reduzir o impacto quando as interrupções são isoladas a serviços discretos. O [Amazon API Gateway](#) permite configurar respostas personalizadas para as APIs REST. Isso permite fornecer mensagens claras e significativas para os consumidores da API quando o API Gateway não puder acessar os serviços de back-end. As mensagens personalizadas também podem ser usadas para dar suporte a notificações e conteúdos de banner sobre a interrupção quando um recurso específico do sistema é danificado devido a interrupções no nível do serviço.

As mensagens diretas são o tipo mais personalizado de mensagens para o cliente. O [Amazon Pinpoint](#) é um serviço gerenciado para comunicações escaláveis de vários canais. O Amazon Pinpoint permite criar campanhas que possam transmitir mensagens amplamente pela base de clientes afetados por SMS, e-mail, mensagem de voz, notificações por push ou canais personalizados definidos por você. Ao gerenciar as mensagens com o Amazon Pinpoint, as campanhas de mensagem são bem-definidas, testáveis e podem ser aplicadas de forma inteligente a segmentos de clientes-alvo. Depois de serem estabelecidas, as campanhas podem ser agendadas ou acionadas por eventos e podem ser facilmente testadas.

Exemplo de clientes

Quando a workload é prejudicada, a Loja UmaEmpresa envia uma notificação por e-mail aos usuários. O e-mail descreve qual funcionalidade da empresa foi prejudicada e fornece uma estimativa realista de quando o serviço será restaurado. Além disso, há uma página de status que mostra informações em tempo real sobre a integridade da workload. O plano de comunicação é testado em um ambiente de desenvolvimento duas vezes ao ano para validar sua eficácia.

Etapas da implementação

1. Determine os canais de comunicação para sua estratégia de mensagens. Considere os aspectos da arquitetura da aplicação e determine a melhor estratégia para fornecer feedback aos clientes. Isso pode incluir uma ou mais das estratégias de orientação descritas, incluindo páginas de erro e de status, respostas de erro de API personalizadas ou mensagens diretas.
2. Elabore páginas de status para a aplicação. Se você determinou que as páginas de status ou de erro personalizadas são adequadas para os clientes, é necessário elaborar o conteúdo e

as mensagens para essas páginas. As páginas de erro explicam aos usuários por que uma aplicação não está disponível, quando ela pode ficar disponível novamente e o que pode ser feito enquanto isso. Se a aplicação usar o Amazon CloudFront, é possível fornecer [respostas de erro personalizadas](#) ou usar o Lambda no Edge para [traduzir erros](#) e reescrever o conteúdo da página. O CloudFront também permite mudar os destinos do conteúdo da aplicação para uma origem de conteúdo estático do [Amazon S3](#) que contém sua página de status da interrupção ou de manutenção.

3. Elabore o conjunto de status de erro de API correto para seu serviço. As mensagens de erro produzidas pelo API Gateway quando ele não consegue acessar os serviços de back-end, além das exceções no nível do serviço, podem não conter mensagens amistosas adequadas para exibição aos usuários finais. Sem precisar fazer alterações no código dos serviços de back-end, é possível configurar as [respostas de erro personalizadas](#) do API Gateway para mapear os códigos de resposta HTTP para mensagens de erro de API selecionadas.
4. Elabore mensagens de uma perspectiva empresarial para que elas sejam relevantes aos usuários finais do sistema e não contenham detalhes técnicos. Considere seu público e alinhe suas mensagens. Por exemplo, você pode conduzir os usuários internos para uma solução alternativa ou um processo manual que utiliza sistemas alternativos. Os usuários externos podem ser solicitados a aguardar até que o sistema seja restaurado ou assinar as atualizações para receber uma notificação quando o sistema for restaurado. Defina mensagens aprovadas para vários cenários, incluindo interrupções não planejadas, manutenção planejada e falhas parciais do sistema quando um recurso específico pode estar danificado ou indisponível.
5. Modele e automatize as mensagens para os clientes. Depois de estabelecer o conteúdo das mensagens, é possível usar o [Amazon Pinpoint](#) ou outras ferramentas para automatizar sua campanha de mensagens. Com o Amazon Pinpoint, é possível criar segmentos de destino de clientes para usuários afetados específicos e transformar as mensagens em modelos. Consulte o [Tutorial do Amazon Pinpoint](#) para entender como configurar uma campanha de mensagens.
6. Evite o acoplamento forte de recursos de mensagens ao sistema voltado para o cliente. Sua estratégia de mensagens não deve depender fortemente de serviços ou armazenamentos de dados do sistema para verificar se é possível enviar mensagens quando ocorrerem interrupções. Considere desenvolver a capacidade de enviar mensagens a mais de [uma região ou zona de disponibilidade](#) para disponibilidade de mensagens. Se você estiver usando os serviços da AWS para enviar mensagens, utilize as operações do plano de dados sobre as [operações do ambiente de gerenciamento](#) para invocar suas mensagens.

Nível de esforço do plano de implementação: alto. Desenvolver um plano de comunicação e os mecanismos para enviá-lo pode exigir um esforço significativo.

Recursos

Práticas recomendadas relacionadas:

- [OPS07-BP03 Usar runbooks para realizar procedimentos](#) – Seu plano de comunicação deve ter um runbook associado a ele para que seus funcionários saibam como responder.
- [OPS11-BP02 Executar análise pós-incidente](#) – Depois de uma interrupção, realize uma análise pós-incidente para identificar mecanismos, a fim de evitar outra interrupção.

Documentos relacionados:

- [Error Handling Patterns in Amazon API Gateway and AWS Lambda](#)(Padrões de tratamento de erros no Amazon API Gateway e no AWS Lambda)
- [Amazon API Gateway responses](#) (Respostas do Amazon API Gateway)

Exemplos relacionados:

- [AWS Health Dashboard](#) (Painel do AWS Health)
- [Summary of the AWS Service Event in the Northern Virginia \(US-EAST-1\) Region](#) (Resumo do evento de serviço da AWS na região Virgínia do Norte (US-EAST-1))

Serviços relacionados:

- [AWS Support](#)
- [Contrato de Cliente da AWS](#)
- [Amazon CloudFront](#)
- [Amazon API Gateway](#)
- [Amazon Pinpoint](#)
- [Amazon S3](#)

OPS10-BP06 Comunicar o status por meio de painéis

Forneça painéis personalizados para seus públicos-alvo (por exemplo, equipes técnicas internas, liderança e clientes) para comunicar o status operacional atual dos negócios e fornecer métricas de interesse.

Você pode criar painéis usando o [Painéis do Amazon CloudWatch](#) em páginas de início personalizáveis no console do CloudWatch. Ao usar serviços de inteligência de negócios, como o [Amazon QuickSight](#), você pode criar e publicar painéis interativos da carga de trabalho e da integridade operacional (por exemplo, taxas de pedidos, usuários conectados e tempos de transação). Crie painéis contendo visualizações em nível de sistema e de negócios de suas métricas.

Antipadrões comuns:

- Mediante solicitação, você executa um relatório sobre a utilização atual da aplicação para a gerência.
- Durante um incidente, você é contatado a cada vinte minutos por um proprietário do sistema preocupado, que deseja saber se ele já foi corrigido.

Benefícios do estabelecimento desta prática recomendada: Ao criar painéis, você permite o acesso por autoatendimento às informações, permitindo que os clientes se informem e determinem se precisam executar ações.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

- Comunicar o status por meio de painéis: forneça painéis personalizados para seus públicos-alvo (por exemplo, equipes técnicas internas, liderança e clientes) para comunicar o status operacional atual dos negócios e fornecer métricas de interesse. Fornecer uma opção de autoatendimento para informações de status reduz a interrupção das solicitações de status de campo pela equipe de operações. Os exemplos incluem os painéis do Amazon CloudWatch e o AWS Health Dashboard.
- [CloudWatch dashboards create and use customized metrics views \(Os painéis do CloudWatch criam e usam visualizações de métricas personalizadas\)](#)

Recursos

Documentos relacionados:

- [Amazon QuickSight](#)
- [CloudWatch dashboards create and use customized metrics views \(Os painéis do CloudWatch criam e usam visualizações de métricas personalizadas\)](#)

OPS10-BP07 Automatizar respostas a eventos

Automatize as respostas aos eventos para reduzir erros causados por processos manuais e garantir respostas rápidas e consistentes.

Existem várias maneiras de automatizar a execução de ações de runbook e manual na AWS. Para responder a um evento de alteração de estado nos seus recursos da AWS, ou de seus próprios eventos personalizados, você deve criar [regras do CloudWatch Events](#) para acionar respostas por meio de alvos do CloudWatch (por exemplo, funções do Lambda, tópicos do Amazon Simple Notification Service (Amazon SNS), tarefas do Amazon ECS e automação do AWS Systems Manager).

Para responder a uma métrica que ultrapassa um limite para um recurso (por exemplo, tempo de espera), você deve criar [alarmes do CloudWatch](#) para executar uma ou mais ações usando as ações do Amazon EC2, as ações do Auto Scaling ou enviar uma notificação para um tópico do Amazon SNS. Se for necessário executar ações personalizadas em resposta a um alarme, chame o Lambda por meio de uma notificação do Amazon SNS. Use o Amazon SNS para publicar notificações de eventos e mensagens de escalação para manter as pessoas informadas.

A AWS também é compatível com sistemas de terceiros por meio das APIs e SDKs de serviço da AWS. Existem várias ferramentas de monitoramento fornecidas por parceiros da AWS e por terceiros que permitem monitoramento, notificações e respostas. Algumas dessas ferramentas são New Relic, Splunk, Loggly, SumoLogic e Datadog.

Mantenha procedimentos manuais críticos disponíveis para uso quando houver falha em procedimentos automatizados.

Antipadrões comuns:

- Um desenvolvedor verifica seu código. Esse evento poderia ter sido usado para iniciar uma compilação e, em seguida, executar testes, mas, em vez disso, nada acontece.

- Sua aplicação registra um erro específico em log antes de parar de funcionar. O procedimento para reiniciar o aplicativo é bem compreendido e pode ter um script. Você pode usar o evento de log para invocar um script e reiniciar o aplicativo. Em vez disso, quando o erro acontece às 3 da manhã de domingo, você é despertado como o recurso de plantão responsável pela correção do sistema.

Benefícios do estabelecimento desta prática recomendada: Ao usar respostas automatizadas a eventos, você reduz o tempo de resposta e limita a introdução de erros oriundos de atividades manuais.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Baixo

Orientações para a implementação

- Automatizar respostas a eventos: automatize respostas a eventos para reduzir erros causados por processos manuais e garantir respostas rápidas e consistentes.
 - [O que é o Amazon CloudWatch Events?](#)
 - [Criação de uma regra do CloudWatch Events que aciona um evento](#)
 - [Criação de uma regra do CloudWatch Events que aciona uma chamada de API da AWS usando o AWS CloudTrail](#)
 - [Exemplos de eventos do CloudWatch Events de serviços compatíveis](#)

Recursos

Documentos relacionados:

- [Recursos do Amazon CloudWatch](#)
- [Exemplos de eventos do CloudWatch Events de serviços compatíveis](#)
- [Criação de uma regra do CloudWatch Events que aciona uma chamada de API da AWS usando o AWS CloudTrail](#)
- [Criação de uma regra do CloudWatch Events que aciona um evento](#)
- [O que é o Amazon CloudWatch Events?](#)

Vídeos relacionados:

- [Build a monitoring plan](#)

Exemplos relacionados:

Evoluir

Evolução é o ciclo contínuo de melhoria ao longo do tempo. Implemente pequenas alterações incrementais frequentes com base nas lições aprendidas com base nas atividades de operações e avalie o êxito delas na obtenção de melhorias.

Para evoluir suas operações ao longo do tempo, você deve ser capaz de:

Tópicos

- [Aprenda, compartilhe e aprimore](#)

Aprenda, compartilhe e aprimore

É essencial que você forneça regularmente tempo para análise das atividades operacionais, análise de falhas, experimentação e aprimoramentos. Quando as coisas falham, você deve garantir que sua equipe, assim como sua comunidade de engenharia maior, aprenda com essas falhas. Você deve analisar falhas para identificar as lições aprendidas e planejar melhorias. Você desejará revisar regularmente suas lições aprendidas com outras equipes para validar suas ideias.

Práticas recomendadas

- [OPS11-BP01 Ter um processo para a melhoria contínua](#)
- [OPS11-BP02 Executar análise pós-incidente](#)
- [OPS11-BP03 Implementar loops de feedback](#)
- [OPS11-BP04 Realizar o gerenciamento de conhecimento](#)
- [OPS11-BP05 Definir motivadores de melhoria](#)
- [OPS11-BP06 Validar insights](#)
- [OPS11-BP07 Fazer análises das métricas de operações](#)
- [OPS11-BP08 Documentar e compartilhar as lições aprendidas](#)
- [OPS11-BP09 Alocar tempo para fazer melhorias](#)

OPS11-BP01 Ter um processo para a melhoria contínua

Avalie sua workload em relação às práticas recomendadas de arquitetura interna e externa. Realize análises da workload pelo menos uma vez ao ano. Priorize as oportunidades de melhoria em sua cadência de desenvolvimento de software.

Resultado desejado:

- Você analisa sua workload em relação às práticas recomendadas de arquitetura pelo menos anualmente.
- As oportunidades de melhoria recebem a mesma prioridade em seu processo de desenvolvimento de software.

Antipadrões comuns:

- Você não realizou uma análise de arquitetura em sua workload desde que foi implantada há vários anos.
- As oportunidades de melhoria recebem uma prioridade mais baixa e permanecem no backlog.
- Não há um padrão para implementar modificações nas práticas recomendadas da organização.

Benefícios do estabelecimento desta prática recomendada:

- Sua workload é mantida atualizada em relação às práticas recomendadas de arquitetura.
- A evolução de sua workload é realizada de forma deliberada.
- Você pode utilizar as práticas recomendadas da organização para melhorar todas as workloads.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

Pelo menos anualmente, você realiza uma análise arquitetônica de sua workload. Usando práticas recomendadas internas e externas, avalie sua workload e identifique oportunidades de melhoria. Priorize as oportunidades de melhoria em sua cadência de desenvolvimento de software.

Exemplo de clientes

Todas as workloads da AnyCompany Retail passam por um processo anual de análise da arquitetura. A empresa desenvolveu a própria lista de verificação de práticas recomendadas que se

aplicam a todas as workloads. Usando o recurso Custom Lens do AWS Well-Architected Tool, foram realizadas análises com a ferramenta e Custom Lens de práticas recomendadas. As oportunidades de melhoria geradas pelas análises recebem prioridade nos sprints de software.

Etapas da implementação

1. Realize análises de arquitetura periódicas de sua workload de produção pelo menos anualmente. Use um padrão de arquitetura documentado que inclua práticas recomendadas específicas da AWS.
 - a. Recomendamos usar seus próprios padrões definidos internamente para essas análises. Se você não tiver um padrão interno, recomendamos usar a AWS Well-Architected Framework.
 - b. Você pode usar o AWS Well-Architected Tool para criar um Custom Lens de suas práticas recomendadas internas e realizar a análise de sua arquitetura.
 - c. Os clientes podem entrar em contato com o arquiteto de soluções da AWS para realizar uma Análise da Well-Architected Framework da workload deles.
2. Priorize as oportunidades de melhoria identificadas durante a análise em seu processo de desenvolvimento de software.

Nível de esforço do plano de implementação: baixo. É possível usar a AWS Well-Architected Framework para realizar sua análise de arquitetura anual.

Recursos

Práticas recomendadas relacionadas:

- [OPS11-BP02 Executar análise pós-incidente](#): análise pós-incidente é outro gerador de itens de melhoria. Insira as lições aprendidas em sua lista interna de práticas recomendadas de arquitetura.
- [OPS11-BP08 Documentar e compartilhar as lições aprendidas](#): à medida que você desenvolve suas próprias práticas recomendadas de arquitetura, compartilhe-as em sua organização.

Documentos relacionados:

- [AWS Well-Architected Tool: Custom lenses](#)
- [AWS Whitepaper sobre Well-Architected: The review process](#) (O processo de revisão)
- [Customize Well-Architected Reviews using Custom Lenses and the AWS Well-Architected Tool](#) (Personalizar as Revisões de Well-Architected com o uso de Custom Lenses e o AWS Well-Architected Tool)

- [Implementing the AWS Well-Architected Custom Lens lifecycle in your organization](#) (Implementar o ciclo de vida do AWS Well-Architected Custom Lens em sua organização)

Vídeos relacionados:

- [Well-Architected Labs - Level 100: Custom Lenses on AWS Well-Architected Tool](#) (Well-Architected Labs: nível 100: Custom Lenses no AWS Well-Architected Tool)

Exemplos relacionados:

- [O AWS Well-Architected Tool](#)

OPS11-BP02 Executar análise pós-incidente

Analise os eventos que afetam o cliente e identifique os fatores que contribuem e as ações preventivas. Use essas informações para desenvolver mitigações para limitar ou evitar recorrência. Desenvolva procedimentos para respostas rápidas e eficazes. Comunique os fatores contribuintes e as ações corretivas conforme apropriado, de acordo com o público-alvo.

Antipadrões comuns:

- Você administra um servidor de aplicativos. Aproximadamente a cada 23 horas e 55 minutos, todas as sessões ativas são encerradas. Você tentou identificar o que está errado no servidor de aplicativos. Você suspeita que possa ser um problema de rede, mas não consegue obter colaboração da equipe da rede, pois ela está muito ocupada para ajudar você. Você não tem um processo predefinido a seguir para obter suporte e coletar as informações necessárias para determinar o que está acontecendo.
- Você teve perda de dados em sua carga de trabalho. Esta é a primeira vez que isso acontece e a causa não é óbvia. Você decide que não é importante porque pode recriar os dados. A perda de dados começa a ocorrer com maior frequência, afetando seus clientes. Isso também coloca uma sobrecarga operacional adicional à medida que você restaura os dados ausentes.

Benefícios do estabelecimento desta prática recomendada: Ter processos predefinidos para determinar componentes, condições, ações e eventos que contribuíram para um incidente permite identificar oportunidades de melhoria.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Alto

Orientações para a implementação

- Usar um processo para determinar os fatores contribuintes: analise todos os incidentes que impactam os clientes. Tenha um processo para identificar e documentar as causas de um incidente para que você possa desenvolver atenuações para limitar ou impedir a recorrência e para desenvolver procedimentos para respostas rápidas e eficazes. Se for apropriado, comunique as causas de forma direcionada para o público-alvo.

OPS11-BP03 Implementar loops de feedback

Os loops de feedback fornecem insights que levem a ações concretas e orientem a tomada de decisões. Crie loops de feedback em seus procedimentos e workloads. Isso ajuda a identificar problemas e áreas que precisam de melhorias. Eles também validam os investimentos feitos em melhorias. Esses loops de feedback são a base para melhorar continuamente sua workload.

Os loops de feedback se enquadram em duas categorias: feedback imediato e análise retrospectiva. O feedback imediato é coletado por meio da avaliação do desempenho e dos resultados das atividades de operações. Esse feedback vem de membros da equipe, clientes ou do resultado automático da atividade. O feedback imediato é recebido de elementos como testes A/B e do envio de novos recursos, e é essencial para antecipar-se à falha.

A análise retrospectiva é realizada regularmente para obter feedback da avaliação de resultados e métricas operacionais ao longo do tempo. Essa retrospectiva ocorre ao final de um sprint, com certa frequência ou após grandes lançamentos ou eventos. Esse tipo de loop de feedback valida investimentos em operações ou na workload. Ele ajuda a medir o sucesso e valida sua estratégia.

Resultado desejado: o feedback imediato e a análise retrospectiva são usados para promover melhorias. Há um mecanismo para obter o feedback de usuários e membros da equipe. A análise retrospectiva é usada para identificar tendências que promovam melhorias.

Antipadrões comuns:

- Você lança um recurso, mas não há uma maneira de receber feedback de clientes sobre ele.
- Depois de investir em melhorias de operações, você não realiza uma retrospectiva para validá-las.
- Você coleta feedback dos clientes, mas não os avalia regularmente.
- Os loops de feedback levam a itens de ação propostos, mas não estão incluídos no processo de desenvolvimento de software.
- Os clientes não recebem feedback sobre as melhorias que propuseram.

Benefícios de estabelecer esta prática recomendada:

- Você pode trabalhar partindo do feedback do cliente para gerar outros recursos.
- A cultura da sua organização pode reagir às mudanças mais rapidamente.
- As tendências são usadas para identificar oportunidades de melhoria.
- As retrospectivas validam os investimentos feitos na workload e nas operações.

Nível de risco exposto se essa prática recomendada não for estabelecida: alto

Orientação para implementação

A implementação dessa prática recomendada significa que você usa tanto o feedback imediato como a análise de retrospectiva. Esses loops de feedback geram melhorias. Há muitos mecanismos para o feedback imediato, incluindo pesquisas, enquetes com clientes ou formulários de feedback. Sua organização também pode usar as retrospectivas para identificar oportunidades de melhoria e validar iniciativas.

Exemplo de cliente

A Loja UmaEmpresa criou um formulário online pelo qual os clientes podem dar feedback ou relatar problemas. Durante as reuniões semanais, o feedback dos usuários é avaliado pela equipe de desenvolvimento de software. O feedback é usado regularmente para conduzir a evolução da plataforma. É feita uma retrospectiva ao final de cada sprint para identificar itens que eles desejam melhorar.

Etapas da implementação

1. Feedback imediato

- Você precisa de um mecanismo para receber feedback de clientes e membros da equipe. Suas atividades de operações também podem ser configuradas para oferecer feedback automático.
- Sua organização precisa de um processo para avaliar esse feedback, determinar o que precisa ser melhorado e programar a melhoria.
- O feedback deve ser adicionado ao seu processo de desenvolvimento de software.
- À medida que você faz melhorias, dê um retorno a quem enviou o feedback.
 - Você pode usar o [AWS Systems Manager OpsCenter](#) para criar e monitorar essas melhorias como [OpsItems](#).

2. Análise retrospectiva

- Faça retrospectivas ao final de um ciclo de desenvolvimento, com certa frequência ou após um grande lançamento.
- Faça uma reunião de retrospectiva com as partes interessadas envolvidas na workload.
- Crie três colunas em um quadro branco ou uma planilha: “Parar”, “Iniciar” e “Manter”.
 - A coluna “Parar” é para o que você deseja que a equipe pare de fazer.
 - A coluna “Iniciar” é para ideias que você deseja começar a fazer.
 - A coluna “Manter” é para os itens que você deseja continuar fazendo.
- Caminhe pela sala e colete o feedback das partes interessadas.
- Priorize o feedback. Atribua ações e partes interessadas aos itens de “Iniciar” e “Manter”.
- Adicione as ações ao processo de desenvolvimento de software e comunique as atualizações de status às partes interessadas à medida que as melhorias são implementadas.

Nível de esforço do plano de implementação: médio. Para implementar essa prática recomendada, você precisa de uma maneira para receber feedback imediato e analisá-lo. Além disso, você precisa estabelecer um processo de análise de retrospectiva.

Recursos

Práticas recomendadas relacionadas:

- [OPS01-BP01 Avaliar as necessidades dos clientes externos](#): loops de feedback são um mecanismo para coletar as necessidades de clientes externos.
- [OPS01-BP02 Avalie as necessidades dos clientes internos](#): as partes interessadas internas podem usar loops de feedback para comunicar necessidades e requisitos.
- [OPS11-BP02 Executar análise pós-incidente](#): a análise pós-incidente é uma forma importante de análise retrospectiva conduzida após os incidentes.
- [OPS11-BP07 Fazer análises das métricas de operações](#): as avaliações das métricas de operações identificam tendências e áreas para melhorias.

Documentos relacionados:

- [7 Pitfalls to Avoid When Building a CCOE \(Sete obstáculos a evitar ao criar um CCoE\)](#)
- [Atlassian Team Playbook - Retrospectives \(Manual da equipe do Atlassian: retrospectivas\)](#)
- [Email Definitions: Feedback Loops \(Definições de e-mail: loops de feedback\)](#)

- [Establishing Feedback Loops Based on the AWS Well-Architected Framework Review \(Como estabelecer loops de feedback com base na avaliação do AWS Well-Architected Framework\)](#)
- [IBM Garage Methodology - Hold a retrospective \(Metodologia IBM Garage: faça uma retrospectiva\)](#)
- [Investopedia – The PDCA Cycle \(Investopédia: o ciclo de PDCA\)](#)
- [Maximizing Developer Effectiveness by Tim Cochran \(Como maximizar a eficácia do desenvolvedor, por Tim Cochran\)](#)
- [Operations Readiness Reviews \(ORR\) Whitepaper - Iteration \(Whitepaper de análises de preparação de operações \(ORR\): iteração\)](#)
- [TIL CSI - Continual Service Improvement \(CSI de TIL: melhoria de serviço contínua\)](#)
- [When Toyota met e-commerce: Lean at Amazon \(Quando a Toyota chegou ao comércio eletrônico: confiança na Amazon\)](#)

Vídeos relacionados:

- [Building Effective Customer Feedback Loops \(Como criar loops de feedback eficazes de clientes\)](#)

Exemplos relacionados:

- [Astuto - Open source customer feedback tool \(Astuto: ferramenta de código aberto de feedback de clientes\)](#)
- [AWS Solutions - QnABot on AWS \(Soluções da AWS: QnABot na AWS\)](#)
- [Fider - A platform to organize customer feedback \(Fider: uma plataforma para organizar feedback de clientes\)](#)

Serviços relacionados:

- [AWS Systems Manager OpsCenter](#)

OPS11-BP04 Realizar o gerenciamento de conhecimento

O gerenciamento de conhecimento ajuda os membros da equipe a encontrar as informações para realizar o trabalho deles. Nas organizações de aprendizagem, as informações são compartilhadas livremente, o que capacita as pessoas. As informações podem ser descobertas ou pesquisadas. As informações são precisas e atualizadas. Os mecanismos existem para criar informações, atualizar

informações existentes e arquivar informações desatualizadas. O exemplo mais comum de uma plataforma de gerenciamento de conhecimento é um sistema de gerenciamento de conteúdo como uma wiki.

Resultado desejado:

- Os membros da equipe têm acesso a informações precisas e em tempo hábil.
- As informações podem ser pesquisadas.
- Existem mecanismos para adicionar, atualizar e arquivar informações.

Antipadrões comuns:

- Não há um armazenamento de conhecimento centralizado. Os membros da equipe gerenciam suas próprias notas nas máquinas locais.
- Você tem uma wiki hospedada pela própria empresa, mas nenhum mecanismo para gerenciar informações, resultando em informações desatualizadas.
- Alguém identifica a ausência de informações, mas não há nenhum processo para solicitar a adição delas à wiki da equipe. Essa pessoa adiciona as informações por conta própria, mas deixa de realizar uma etapa, resultando em uma interrupção.

Benefícios do estabelecimento desta prática recomendada:

- Os membros da equipe são capacitados, pois as informações são compartilhadas livremente.
- Os novos membros da equipe passam pelo processo de integração mais rapidamente, pois a documentação está atualizada e pode ser pesquisada.
- As informações são precisas, levam a ações concretas e são enviadas em tempo hábil.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

O gerenciamento de conhecimento é uma faceta importante das organizações de aprendizagem. Para começar, é necessário ter um repositório central para armazenar seu conhecimento (como um exemplo comum, uma wiki hospedada pela própria empresa). É necessário desenvolver processos para adicionar, atualizar e arquivar conhecimento. Desenvolva padrões para o que deve ser documentado e permita que todos contribuam.

Exemplo de clientes

A Loja UmaEmpresa hospeda uma wiki interna em que todo o conhecimento é armazenado. Os membros da equipe são incentivados a adicionar informações na base de conhecimento à medida que realizam suas tarefas diárias. Trimestralmente, uma equipe multifuncional avalia quais páginas estão mais desatualizadas e determina se elas devem ser arquivadas ou atualizadas.

Etapas da implementação

1. Comece identificando o sistema de gerenciamento de conteúdo em que o conhecimento será armazenado. Obtenha o consentimento das partes interessadas em sua organização.
 - a. Se você não tiver um sistema de gerenciamento de conteúdo, considere desenvolver uma wiki hospedada pela própria empresa ou usar um repositório de controle de versão como ponto de partida.
2. Desenvolva runbooks para adicionar, atualizar e arquivar informações. Instrua a equipe sobre esses processos.
3. Identifique quais conhecimentos devem ser armazenados no sistema de gerenciamento de conteúdo. Comece com atividades diárias (runbooks e manuais) que os membros da equipe realizam. Trabalhe com as partes interessadas para priorizar qual conhecimento deve ser adicionado.
4. Periodicamente, trabalhe com as partes interessadas para identificar informações desatualizadas e archive-as ou atualize-as.

Nível de esforço do plano de implementação: médio. Se você não tiver um sistema de gerenciamento de conteúdo, defina uma wiki hospedada pela própria empresa ou um repositório de documentos com controle de versão.

Recursos

Práticas recomendadas relacionadas:

- [OPS11-BP08 Documentar e compartilhar as lições aprendidas](#) – O gerenciamento de conhecimento facilita o compartilhamento de informações sobre as lições aprendidas.

Documentos relacionados:

- [Atlassian: gerenciamento do conhecimento](#)

Exemplos relacionados:

- [DokuWiki](#)
- [Gollum](#)
- [MediaWiki](#)
- [Wiki.js](#)

OPS11-BP05 Definir motivadores de melhoria

Identifique os condutores de melhoria para ajudá-lo a avaliar e priorizar as oportunidades.

Na AWS, é possível agregar os logs de todas as suas atividades operacionais, workloads e infraestrutura para criar um histórico de atividades detalhado. Assim, é possível usar as ferramentas da AWS para analisar as operações e a integridade da workload ao longo do tempo (por exemplo, identificar tendências, correlacionar eventos e atividades a resultados e comparar e contrastar ambientes e sistemas) para revelar oportunidades de melhoria com base em seus motivadores.

Use o CloudTrail para rastrear a atividade da API (por meio do AWS Management Console, da CLI, de SDKs e de APIs) para saber o que está acontecendo nas suas contas. Rastreie as atividades de implantação das ferramentas do desenvolvedor da AWS com o CloudTrail e o CloudWatch. Isso adicionará um histórico detalhado das atividades de suas implantações e seus resultados aos dados de logs do CloudWatch Logs.

[Exporte seus dados de log para o Amazon S3](#) para armazenamento de longo prazo. Com o uso do [AWS Glue](#), você descobre e prepara seus dados de log no Amazon S3 para análise. Use [Amazon Athena](#), por meio de sua integração nativa com o AWS Glue, para analisar os dados de logs. Use uma ferramenta de business intelligence, como o [Amazon QuickSight](#), para visualizar, explorar e analisar os dados.

Antipadrões comuns:

- Você tem um script que funciona, mas não é elegante. Você investe tempo para reescrevê-lo. Agora, ele é uma obra de arte.
- Sua startup está tentando obter outro conjunto de financiamento de um capitalista de risco. Ele quer que você demonstre conformidade com o PCI DSS. Você quer deixá-lo contente, então documenta sua conformidade e perde uma data de entrega para um cliente, perdendo esse cliente. Não foi algo errado, mas agora você se pergunta se foi o certo a se fazer.

Benefícios do estabelecimento desta prática recomendada: Ao determinar os critérios que você deseja implantar para melhorar, é possível minimizar o impacto das motivações baseadas em eventos ou investimentos emocionais.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

- Compreender as motivações para melhoria: só faça alterações em um sistema quando o resultado desejado for suportado.
 - Capacidades desejadas: avalie as capacidades e os recursos desejados ao avaliar oportunidades de melhoria.
 - [Novidades da AWS](#)
 - Problemas inaceitáveis: avalie problemas, bugs e vulnerabilidades inaceitáveis ao avaliar oportunidades de melhoria.
 - [Boletins de segurança mais recentes da AWS](#)
 - [AWS Trusted Advisor](#)
 - Requisitos de conformidade: avalie as atualizações e alterações necessárias para manter a conformidade com a regulamentação e com a política, ou para permanecer sob o suporte de terceiros ao analisar as oportunidades de melhoria.
 - [Conformidade da AWS](#)
 - [Programas de conformidade da AWS](#)
 - [Notícias recentes sobre conformidade da AWS](#)

Recursos

Documentos relacionados:

- [Amazon Athena](#)
- [Amazon QuickSight](#)
- [Conformidade da AWS](#)
- [Notícias recentes sobre conformidade da AWS](#)
- [Programas de conformidade da AWS](#)
- [AWS Glue](#)
- [Boletins de segurança mais recentes da AWS](#)

- [AWS Trusted Advisor](#)
- [Exporte seus dados de log para o Amazon S3](#)
- [Novidades da AWS](#)

OPS11-BP06 Validar insights

Revise os resultados e as respostas da análise com equipes multifuncionais e proprietários de negócios. Use essas revisões para estabelecer um entendimento comum, identificar impactos adicionais e determinar cursos de ação. Ajuste as respostas conforme apropriado.

Antipadrões comuns:

- Você vê que a utilização da CPU está em 95% em um sistema e prioriza encontrar uma maneira de reduzir a carga no sistema. Você determina que a melhor ação é expandir. O sistema é um transcodificador e foi dimensionado para ser executado com 95% de utilização da CPU o tempo todo. O proprietário do sistema poderia ter explicado a situação se você tivesse entrado em contato com ele. Seu tempo foi perdido.
- Um proprietário do sistema sustenta que o sistema é de missão crítica. O sistema não foi colocado em um ambiente de alta segurança. Para melhorar a segurança, você implementa os controles de detecção e prevenção adicionais necessários para sistemas de missão crítica. Você notifica o proprietário do sistema de que o trabalho foi concluído e que ele será cobrado pelos recursos adicionais. Na discussão após essa notificação, o proprietário do sistema aprende que há uma definição formal para sistemas de missão crítica que o sistema dele não atende.

Benefícios do estabelecimento desta prática recomendada: Ao validar insights com proprietários de empresas e especialistas no assunto, você pode estabelecer um entendimento comum e orientar de maneira mais eficaz a melhoria.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Médio

Orientações para a implementação

- Validar insights: envolva-se com proprietários de empresas e especialistas no assunto para garantir que haja entendimento e concordância comuns sobre o significado dos dados coletados. Identifique preocupações adicionais, possíveis impactos e determine as ações.

OPS11-BP07 Fazer análises das métricas de operações

Realize regularmente análises retrospectivas das métricas de operações com participantes de equipes cruzadas de diferentes áreas do negócio. Use essas análises para identificar oportunidades de melhorias e possíveis ações e compartilhar as lições aprendidas.

Procure oportunidades para melhorar em todos os seus ambientes (por exemplo, desenvolvimento, teste e produção).

Antipadrões comuns:

- Houve uma promoção de varejo significativa que foi interrompida por sua janela de manutenção. A empresa continua sem saber que existe uma janela de manutenção padrão que pode ser atrasada se houver outros eventos que afetam os negócios.
- Você sofreu uma interrupção prolongada devido ao uso de uma biblioteca com bugs geralmente utilizada em sua organização. Desde então, você migrou para uma biblioteca confiável. As outras equipes da organização não sabem que estão em risco. Se você se reunisse regularmente e analisasse esse incidente, eles ficariam conscientes do risco.
- A performance do transcodificador tem diminuído constantemente e está afetando a equipe de mídia. Ainda não é algo terrível. Você não terá a oportunidade de descobrir até que seja ruim o suficiente para causar um incidente. Se você analisasse as métricas de operações com a equipe de mídia, haveria uma oportunidade para que a mudança nas métricas e a experiência deles fossem reconhecidas e o problema fosse resolvido.
- Você não está analisando a satisfação dos SLAs do cliente. Você está tendendo a não cumprir os SLAs de seus clientes. Há penalidades financeiras relacionadas ao não cumprimento de SLAs dos clientes. Se você se reunisse regularmente para analisar as métricas desses SLAs, teria a oportunidade de reconhecer e resolver o problema.

Benefícios do estabelecimento desta prática recomendada: Ao realizar reuniões regularmente para analisar métricas, eventos e incidentes de operações, você mantém um entendimento comum entre as equipes, compartilha as lições aprendidas e pode priorizar e direcionar melhorias.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Médio

Orientações para a implementação

- Análises das métricas das operações: execute regularmente análises retrospectivas das métricas de operações com participantes de equipes de diferentes áreas do negócio. Envolver as partes

interessadas, incluindo as equipes de negócios, desenvolvimento e operações, para validar suas descobertas de feedback imediato e análise retrospectiva e para compartilhar as lições aprendidas. Use suas ideias para identificar oportunidades de melhoria e possíveis cursos de ação.

- [Amazon CloudWatch](#)
- [Uso de métricas do Amazon CloudWatch](#)
- [Publicar métricas personalizadas](#)
- [Referência de métricas e de dimensões do Amazon CloudWatch](#)

Recursos

Documentos relacionados:

- [Amazon CloudWatch](#)
- [Referência de métricas e de dimensões do Amazon CloudWatch](#)
- [Publicar métricas personalizadas](#)
- [Uso de métricas do Amazon CloudWatch](#)

OPS11-BP08 Documentar e compartilhar as lições aprendidas

Documente e compartilhe as lições aprendidas das atividades operacionais, para que possa usá-las internamente e entre equipes.

Você deve compartilhar o que suas equipes aprendem para aumentar os benefícios em toda a organização. Você desejará compartilhar informações e recursos para evitar erros que podem ser evitados e facilitar os esforços de desenvolvimento. Isso permitirá que você se concentre no fornecimento dos recursos desejados.

Use o AWS Identity and Access Management (IAM) para definir permissões que permitem acesso controlado aos recursos que você deseja compartilhar dentro e entre contas. Você deve usar os repositórios do AWS CodeCommit com controle de versão para compartilhar bibliotecas de aplicativos, procedimentos com script, documentações de procedimentos e outras documentações do sistema. Compartilhe seus padrões de computação partilhando o acesso às suas AMIs e autorizando o uso de suas funções do Lambda entre contas. Você também deve compartilhar seus padrões de infraestrutura como modelos do AWS CloudFormation.

Por meio de APIs e SDKs da AWS, é possível integrar ferramentas e repositórios externos e de terceiros (por exemplo, GitHub, BitBucket e SourceForge). Ao compartilhar o que você aprendeu e desenvolveu, tenha cuidado para estruturar as permissões para garantir a integridade dos repositórios compartilhados.

Antipadrões comuns:

- Você sofreu uma interrupção prolongada devido ao uso de uma biblioteca com bugs geralmente utilizada em sua organização. Desde então, você migrou para uma biblioteca confiável. As outras equipes em sua organização não sabem que estão em risco. Se você documentasse e compartilhasse sua experiência com essa biblioteca, eles ficariam cientes do risco.
- Você identificou um caso de borda em um microsserviço compartilhado internamente que causa a queda das sessões. Você atualizou suas chamadas para o serviço para evitar esse caso extremo. As outras equipes da organização não sabem que estão em risco. Se você documentasse e compartilhasse sua experiência com essa biblioteca, eles ficariam cientes do risco.
- Você encontrou uma maneira de reduzir significativamente os requisitos de utilização da CPU para um dos seus microsserviços. Você não sabe se alguma outra equipe poderia aproveitar essa técnica. Se você documentasse e compartilhasse sua experiência com essa biblioteca, eles teriam a oportunidade de aproveitá-la.

Benefícios do estabelecimento desta prática recomendada: Compartilhe as lições aprendidas para apoiar melhorias e maximizar os benefícios da experiência.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Baixo

Orientações para a implementação

- Documentar e compartilhar as lições aprendidas: tenha procedimentos para documentar as lições aprendidas com a execução de atividades operacionais e análises retrospectivas, para que possam ser usadas por outras equipes.
 - Compartilhar lições aprendidas: tenha procedimentos para compartilhar as lições aprendidas e os artefatos associados entre as equipes. Por exemplo, compartilhe procedimentos atualizados, orientações, governança e práticas recomendadas por meio de um wiki acessível. Compartilhe scripts, códigos e bibliotecas por meio de um repositório comum.
 - [Delegação de acesso ao ambiente da AWS](#)
 - [Compartilhar um repositório do AWS CodeCommit](#)
 - [Fácil autorização das funções do AWS Lambda](#)

- [Compartilhamento de uma AMI com contas específicas da AWS](#)
- [Acelerar o compartilhamento de modelos com uma URL do designer do AWS CloudFormation](#)
- [Usar o AWS Lambda com o Amazon SNS](#)

Recursos

Documentos relacionados:

- [Fácil autorização das funções do AWS Lambda](#)
- [Compartilhar um repositório do AWS CodeCommit](#)
- [Compartilhamento de uma AMI com contas específicas da AWS](#)
- [Acelerar o compartilhamento de modelos com uma URL do designer do AWS CloudFormation](#)
- [Usar o AWS Lambda com o Amazon SNS](#)

Vídeos relacionados:

- [Delegação de acesso ao ambiente da AWS](#)

OPS11-BP09 Alocar tempo para fazer melhorias

Dedique tempo e recursos em seus processos para possibilitar melhorias incrementais contínuas.

Na AWS, é possível criar duplicatas temporárias de ambientes, reduzindo o risco, o esforço e o custo da experimentação e dos testes. Esses ambientes duplicados podem ser usados para testar as conclusões de sua análise, experimentar e desenvolver e testar as melhorias planejadas.

Antipadrões comuns:

- Há um problema de performance conhecido no servidor de aplicativos. Ele é adicionado ao backlog por trás de cada implementação de recurso planejada. Se a taxa de adição de recursos planejados permanecer constante, o problema de performance nunca será resolvido.
- Para oferecer suporte à melhoria contínua, você aprova administradores e desenvolvedores usando todo o tempo extra para selecionar e implementar melhorias. Nenhuma melhoria é concluída.

Benefícios do estabelecimento desta prática recomendada: Ao dedicar tempo e recursos em seus processos, você possibilita melhorias incrementais contínuas.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: Baixo

Orientações para a implementação

- Alocar tempo para fazer melhorias: dedique tempo e recursos em seus processos para possibilitar melhorias incrementais contínuas. Implemente alterações para melhorar e avaliar os resultados para determinar o sucesso. Se os resultados não satisfizerem as metas e a melhoria ainda for uma prioridade, siga cursos de ação alternativos.

Conclusão

A excelência operacional é um esforço contínuo e iterativo.

Configure sua organização para o êxito com metas compartilhadas. Garanta que todos entendam sua parte na obtenção de resultados empresariais e como eles afetam a capacidade de êxito de outras pessoas. Dê suporte aos membros da equipe para que eles possam oferecer suporte aos resultados empresariais.

Todo evento e toda falha operacional devem ser tratados como uma oportunidade para melhorar as operações de sua arquitetura. Ao compreender as necessidades de suas cargas de trabalho, predefinir runbooks para atividades rotineiras e manuais para orientar a resolução de problemas, usar as operações como recursos de código na AWS e manter a consciência da situação, suas operações estarão prontas e capazes de responder com mais eficiência quando ocorrerem incidentes.

Ao focar na melhoria incremental com base nas prioridades operacionais e nas lições aprendidas com a resposta a eventos e a análise retrospectiva, você permitirá o êxito de seus negócios, aumentando a eficiência e a eficácia das operações.

A AWS se esforça para ajudá-lo a criar e operar arquiteturas que maximizam a eficiência enquanto você cria implantações altamente responsivas e adaptáveis. Para aumentar a excelência operacional de cargas de trabalho, você deve usar as melhores práticas discutidas neste documento.

Colaboradores

- Rich Boyd, líder do pilar Excelência operacional, Well-Architected, Amazon Web Services
- Jon Steele, arquiteto de soluções, Well-Architected, Amazon Web Services
- Ryan King, gerente técnico de programas sênior, Amazon Web Services
- Chris Kunselman, consultor, Amazon Web Services
- Peter Mullen, consultor, Amazon Web Services
- Brian Quinn, consultor sênior, Amazon Web Services
- David Stanley, líder do modelo operacional de nuvem, Amazon Web Services
- Chris Kozlowski, gerente técnico de contas especialista sênior, suporte empresarial da Amazon Web Services
- Alex Livingstone, arquiteto de soluções chefe especialista, operações em nuvem, Amazon Web Services
- Paul Moran, tecnólogo-chefe, suporte empresarial, Amazon Web Services
- Peter Mullen, consultor, serviços profissionais, Amazon Web Services
- Chris Pates, gerente técnico de contas especialista sênior, suporte empresarial, Amazon Web Services
- Arvind Raghunathan, gerente técnico de contas especialista-chefe, suporte empresarial da Amazon Web Services
- Ben Mergen, arquiteto sênior de soluções líder de custos da Amazon Web Services

Leitura adicional

Para obter orientações adicionais, consulte as seguintes fontes:

- [AWS Well-Architected Framework](#)
- [Centro de Arquitetura da AWS](#)

Revisões do documento

Para ser notificado sobre atualizações deste whitepaper, inscreva-se no RSS feed.

Alteração	Descrição	Data
Grande atualização e consolidação de conteúdo	<p>O conteúdo foi atualizado e consolidado em várias áreas de práticas recomendadas. Duas áreas de práticas recomendadas (OPS 04 e OPS 08) foram reescritas com novo conteúdo e foco.</p> <p>As práticas recomendadas foram atualizadas e consolidadas nas seguintes áreas: Design das operações, Mitigar riscos de implantação e Compreensão da integridade operacional. A área de práticas recomendadas OPS 04 foi atualizada para Implementar a observabilidade. A área de práticas recomendadas OPS 08 foi atualizada para Utilizar a observabilidade da workload.</p>	October 3, 2023
Atualizações para o novo Framework	Práticas recomendadas atualizadas com orientações prescritivas e novas práticas recomendadas adicionadas.	April 10, 2023
Whitepaper atualizado	Práticas recomendadas atualizadas com novas	December 15, 2022

	orientações para implementação.	
Whitepaper atualizado	Práticas recomendadas ampliadas e planos de melhoria adicionados.	October 20, 2022
Atualização secundária	Pequena atualização editorial.	August 8, 2022
Whitepaper atualizado	Atualizações para refletir novos serviços e recursos da AWS e as práticas recomendadas recentes.	February 2, 2022
Atualização secundária	Pilar Sustentabilidade adicionado à introdução.	December 2, 2021
Atualizações para o novo Framework	Atualizações para refletir novos serviços e recursos da AWS e as melhores práticas recentes.	July 8, 2020
Whitepaper atualizado	Atualizações para refletir novos serviços e recursos da AWS e referências atualizadas.	July 1, 2018
Publicação inicial	Publicação do pilar Excelência operacional: AWS Well-Architected Framework.	November 1, 2017