



Aplicação do AWS Well-Architected Framework aos aplicativos da Amazon WorkSpaces

AWS Orientação prescritiva



AWS Orientação prescritiva: Aplicação do AWS Well-Architected Framework aos aplicativos da Amazon WorkSpaces

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

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

Table of Contents

Introdução	1
Público-alvo	1
Objetivos	2
Pilar Excelência operacional	3
Organize equipes em torno dos resultados comerciais	3
Implemente a observabilidade para obter insights acionáveis	4
Automatize com segurança sempre que possível	5
Faça mudanças frequentes, pequenas e reversíveis	7
Refine os procedimentos operacionais com frequência	8
Antecipe a falha	9
Aprenda com todos os eventos e métricas operacionais	10
Use serviços gerenciados	11
Pilar Segurança	12
Implemente uma base sólida de identidade	12
Mantenha a rastreabilidade	13
Aplique segurança em todas as camadas	14
Automatize as melhores práticas de segurança	15
Mantenha as pessoas longe dos dados	16
Prepare-se para eventos de segurança	16
Pilar Confiabilidade	18
Recuperação automática de falhas	18
Testar os procedimentos de recuperação	19
Dimensione horizontalmente para aumentar a disponibilidade da carga de trabalho agregada ...	19
Pare de adivinhar a capacidade	20
Gerencie mudanças por meio da automação	20
Pilar Eficiência de performance	21
Democratize tecnologias avançadas	21
Torne-se global em minutos	22
Use arquiteturas sem servidor	22
Experimente com mais frequência	23
Considere a simpatia mecânica	23
Pilar Otimização de custos	25
Implementar o gerenciamento financeiro da nuvem	25
Adicionar um modelo de consumo	25

Meça a eficiência geral	26
Pare de gastar dinheiro em levantamento de peso indiferenciado	26
Analise e atribua despesas	27
Pilar Sustentabilidade	28
Análise do seu impacto	28
Estabeleça metas de sustentabilidade	28
Maximize a utilização	29
Antecipe e adote ofertas de hardware e software novas e mais eficientes	29
Serviços gerenciados usados	30
Reduza o impacto posterior de suas cargas de trabalho na nuvem	30
Recursos	31
AWS documentação	31
AWS postagens no blog	31
Histórico do documento	33
Glossário	34
#	34
A	35
B	38
C	40
D	43
E	48
F	50
G	52
H	53
eu	54
L	57
M	58
O	62
P	65
Q	68
R	68
S	71
T	75
U	77
V	77
W	78

Z	79
.....	lxxx

Aplicação do AWS Well-Architected Framework aos aplicativos da Amazon WorkSpaces

Mohamed Wali, Amazon Web Services

Julho de 2025 ([histórico do documento](#))

[Este guia aborda as melhores práticas para aplicar o AWS Well-Architected Framework ao usar o Amazon Applications. WorkSpaces](#) WorkSpaces O Applications é um serviço de streaming de aplicativos totalmente gerenciado que permite transmitir aplicativos de desktop aos usuários sem precisar reescrevê-los.

O AWS Well-Architected Framework ajuda os arquitetos de nuvem a criar infraestruturas seguras, de alto desempenho, resilientes e eficientes para uma variedade de aplicativos e cargas de trabalho. Ele também fornece uma abordagem consistente para usuários e AWS parceiros avaliarem arquiteturas e implementarem projetos escaláveis.

O AWS Well-Architected Framework é construído em torno de seis pilares:

- Excelência operacional
- Segurança
- Confiabilidade
- Eficiência de desempenho
- Otimização de custos
- Sustentabilidade

Este guia discute como esses pilares e as melhores práticas se aplicam ao uso WorkSpaces de aplicativos.

Público-alvo

Este guia é para:

- Arquitetos e engenheiros de nuvem que projetam e implementam soluções de WorkSpaces aplicativos e precisam garantir que suas arquiteturas sigam as melhores práticas do AWS Well-Architected Framework.

- Equipes de operações de TI que gerenciam e mantêm ambientes de WorkSpaces aplicativos; lidam com gerenciamento, escalonamento e monitoramento de frotas; e precisam otimizar custos e desempenho.
- Organizações ou empresas que estão considerando ou já usam WorkSpaces aplicativos, desejam transmitir aplicativos de desktop para seus usuários e precisam criar infraestruturas seguras, de alto desempenho, resilientes e eficientes.

Objetivos

Seguir as melhores práticas deste guia ajuda você a:

- Crie uma infraestrutura segura, de alto desempenho, resiliente e eficiente para streaming de aplicativos de desktop no. Nuvem AWS
- Aplique uma abordagem consistente ao avaliar arquiteturas de WorkSpaces aplicativos e implementar projetos escaláveis.

Pilar Excelência operacional

A excelência operacional (OE) representa a dedicação à criação de soluções de software de alta qualidade que atendam e superem consistentemente as expectativas dos usuários. O [pilar de excelência operacional](#) do AWS Well-Architected Framework engloba estratégias comprovadas para organização eficaz de equipes, design robusto de carga de trabalho, operações eficientes em grande escala e adaptação perfeita às mudanças nos requisitos ao longo do tempo. Ao aderir a esses princípios, as organizações podem garantir que seus sistemas permaneçam resilientes, com desempenho e alinhados às necessidades comerciais em evolução.

Principais áreas de foco para aplicar esse pilar ao seu ambiente de streaming de WorkSpaces aplicativos:

- Monitoramento e observabilidade
- Automação e DevOps
- Procedimentos operacionais e documentação
- Support e gerenciamento de incidentes

Organize equipes em torno dos resultados comerciais

Crie um modelo operacional alinhado à nuvem com forte compromisso de liderança, em que as metas de negócios e os principais indicadores de desempenho (KPIs) impulsionem a transformação organizacional por meio de pessoas, processos e tecnologia otimizados.

- Estrutura da equipe. Estabeleça equipes dedicadas que se alinhem aos resultados do streaming de aplicativos. Por exemplo:
 - A equipe de gerenciamento de imagens é responsável pelo empacotamento de aplicativos e pela otimização de imagens.
 - A equipe de operações da frota gerencia a capacidade, o desempenho e o dimensionamento.
 - A equipe de experiência do usuário lida com o suporte e a satisfação do usuário final.
- KPIs e métricas. Defina e acompanhe métricas alinhadas aos negócios, como:
 - Taxas de disponibilidade de aplicativos
 - Hora de implantar novos aplicativos
 - Custo por hora de streaming de aplicativos

- Modelo operacional. Crie processos claros para:
 - Integração e atualizações de aplicativos
 - Gerenciamento da capacidade da frota
 - Provisionamento de acesso de usuários
 - Resposta e resolução de incidentes

Implemente a observabilidade para obter insights acionáveis

Implemente monitoramento e observabilidade abrangentes para monitorar a integridade KPIs da carga de trabalho. Esse princípio permite decisões baseadas em dados e melhorias proativas em desempenho, confiabilidade e custo.

- Implemente o monitoramento de desempenho. Configure CloudWatch a [Amazon](#) para:
 - Garanta capacidade suficiente para atender à demanda. Por exemplo, você pode usar as seguintes métricas:
 - `AvailableCapacity` para monitorar as instâncias de streaming disponíveis
 - `InUseCapacity` para rastrear instâncias usadas atualmente
 - `CapacityUtilization` para monitorar a porcentagem de uso da frota
 - Monitore a experiência e o desempenho do usuário.
 - Identifique e resolva problemas de serviço imediatamente.
- Acompanhe e analise os relatórios de uso de WorkSpaces aplicativos.
- Capture e analise os registros do aplicativo. Para obter mais informações, consulte as postagens do AWS blog [Usando o Kinesis Agent para Linux para transmitir registros de WorkSpaces aplicativos em aplicativos](#) e Usando o [Kinesis Agent para Microsoft Windows para armazenar registros de eventos de WorkSpaces aplicativos do Windows](#).
- Monitore métricas e eventos de WorkSpaces aplicativos por meio de notificações de bate-papo. Para obter mais informações, consulte a postagem do AWS blog [Monitore e automatize a computação do usuário AWS final \(EUC\) com o Chatbot AWS](#).
- Habilite o gerenciamento proativo de sessões por meio de dicas visuais. Para obter mais informações, consulte a postagem do AWS blog [Exibir a expiração da sessão e um cronômetro de contagem regressiva nos aplicativos da Amazon WorkSpaces](#).

- Crie visualizações para padrões e tendências de uso. Para obter mais informações, consulte a postagem do AWS blog [Ingeste e visualize os relatórios de uso WorkSpaces dos aplicativos da Amazon no Amazon OpenSearch Service](#).
- Utilize o kit de ferramentas EUC para monitorar sessões ativas, rastrear o inventário da frota e gerar relatórios de sessão (exportação de CSV). Para obter mais informações, consulte a postagem do AWS blog [Use o kit de ferramentas EUC para gerenciar os WorkSpaces aplicativos da Amazon e a Amazon](#). WorkSpaces

Automatize com segurança sempre que possível

Aplice os princípios de infraestrutura como código (IaC) para automatizar todos os aspectos de suas operações de carga de trabalho. Use grades de proteção para ajudar a garantir uma execução segura e consistente e, ao mesmo tempo, reduzir a intervenção manual.

- Automatize a criação e a configuração de imagens de WorkSpaces aplicativos usando a CLI do Image Assistant. Para obter mais informações, consulte [Crie sua imagem do Amazon WorkSpaces Applications programaticamente usando as operações da CLI do Image Assistant](#) na documentação de aplicativos. WorkSpaces
 - Instalação do aplicativo: use a CLI do Image Assistant para automatizar a instalação de aplicativos durante a criação da imagem.
 - Criação de imagem: crie imagens de WorkSpaces aplicativos de forma programática usando os comandos CLI do Image Assistant.
 - Gerenciamento de configuração: automatize a configuração das configurações padrão do aplicativo e dos parâmetros de inicialização.
- Automatize a personalização das imagens dos WorkSpaces aplicativos. Para obter mais informações, consulte a postagem do AWS blog [Criar automaticamente imagens personalizadas de WorkSpaces aplicativos do Windows](#).
- Aplique o IaC para implantar a infraestrutura e os componentes do aplicativo para WorkSpaces aplicativos. Para obter mais informações, consulte a postagem do AWS blog [Automação da infraestrutura e implantação de aplicativos para Amazon WorkSpaces Applications with Terraform](#).
- Implemente processos automatizados para gerenciamento de frotas, incluindo:
 - Dimensionamento da frota com base na demanda. Configure políticas de escalabilidade automática para ajustar automaticamente a capacidade da frota com base nas métricas de

utilização. Para obter mais informações, consulte a postagem do AWS blog [Use AWS Lambda para ajustar etapas e limites de escalabilidade para aplicativos da Amazon WorkSpaces](#).

- Atualizações de imagens básicas. Beneficie-se das atualizações automáticas da imagem base dos WorkSpaces aplicativos fornecida pelo AWS.
- Otimização da capacidade. Configure limites de escalabilidade automatizados para otimizar o uso de recursos com base nos padrões de demanda.
- Configure grades de proteção para automatizar os controles de segurança:
 - Limites máximos de tamanho da frota. Estabeleça limites superiores na capacidade da frota para evitar o excesso de provisionamento.
 - Configuração da política de escalabilidade. Implemente políticas de escalabilidade por etapas ou rastreamento de metas com limites apropriados.
 - Cotas de serviço. Use cotas AWS de serviço como limites incorporados para evitar a alocação excessiva de recursos.
 - Proteção ampliada. Configure a proteção escalável para evitar a remoção de instâncias ativas durante eventos de escalabilidade.
- Execute testes e validação, incluindo testes de criação de imagens, frota e integração.
 - Teste do construtor de imagens:
 - Teste os aplicativos diretamente na interface do criador de imagens.
 - Verifique o lançamento e a funcionalidade do aplicativo.
 - Teste as configurações e configurações do usuário.
 - Valide a compatibilidade do aplicativo.
 - Teste de frota:
 - Teste sessões de streaming de diferentes dispositivos clientes.
 - Verifique os direitos e o acesso do usuário.
 - Valide o desempenho do aplicativo.
 - Teste a experiência do usuário em elementos e operações, como prancheta, transferência de arquivos e impressão.
 - Teste de integração:
 - Teste a autenticação baseada no Active Directory ou no SAML 2.0.
 - Teste as pastas pessoais e o armazenamento persistente.
 - Teste os direitos do aplicativo.

- Teste o redirecionamento do dispositivo USB (se configurado).
- Use o gerenciador de WorkSpaces aplicativos para automatizar o empacotamento e a implantação de aplicativos. Para obter mais informações, consulte a postagem do AWS blog [Simplifique a integração de aplicativos com o gerenciador de aplicativos da Amazon WorkSpaces](#) Applications.
- Automatize a implantação de novas versões de aplicativos usando pipelines de integração contínua e entrega contínua (CI/CD). Para obter mais informações, consulte a postagem do AWS blog [Screening Eagle: Optimize CI/CD and end user experience in Amazon WorkSpaces](#) Applications.

Faça mudanças frequentes, pequenas e reversíveis

Crie cargas de trabalho escaláveis e pouco acopladas que possibilitem implantações automatizadas frequentes e de pequena escala com risco mínimo e recursos fáceis de reversão.

- Para atualizações de imagens, use a criação de imagens versionadas e atualizações incrementais.
 - Criação de imagem versionada:
 - Crie novas imagens para cada conjunto de alterações usando um construtor de imagens.
 - Mantenha várias versões de imagem para suportar cenários de reversão.
 - Use [estratégias de AWS marcação](#) para rastrear versões e atributos de imagens.
 - Atualizações incrementais:
 - Faça pequenas alterações incrementais nos aplicativos ou nas configurações.
 - Teste minuciosamente as atualizações no criador de imagens antes de criar uma nova imagem.
 - Documente todas as alterações que você fez em cada nova versão da imagem.
- Para atualizações da frota de controle:
 - Crie novas frotas com imagens atualizadas para testes.
 - Modifique os atributos da frota existente sem interromper as sessões ativas.
- Estabeleça procedimentos de gerenciamento de mudanças para documentação, protocolos de teste, fluxos de trabalho de aprovação e processos de monitoramento.
 - Documentação:
 - Mantenha registros de alterações detalhados para todas as atualizações de imagem e frota.
 - Documente os procedimentos e os resultados dos testes para cada alteração.

- Use [AWS CloudTrail](#) para rastrear e auditar alterações na configuração.
- Protocolos de teste:
 - Estabeleça um processo de teste abrangente para todas as mudanças.
 - Inclua testes de funcionalidade, desempenho e experiência do usuário do aplicativo.
 - Faça testes no criador de imagens antes de criar novas imagens.
 - Realize testes adicionais em frotas que não são de produção antes da implantação completa.
- Fluxos de trabalho de aprovação:
 - Implemente um processo de aprovação para mudanças nos ambientes de produção.
 - Defina critérios para mudanças que exigem aprovação versus atualizações padrão.
 - Estabeleça funções e responsabilidades para aprovação de mudanças.
- Monitoramento e validação:
 - Use CloudWatch a [Amazon](#) para monitorar o desempenho da frota e do aplicativo após as mudanças.
 - Configure alertas para as principais métricas para identificar rapidamente os problemas após as atualizações.
 - Realize análises pós-implantação para validar o sucesso da mudança e coletar informações.

Refine os procedimentos operacionais com frequência

Melhore continuamente os procedimentos operacionais por meio de revisões regulares, atualizações e engajamento da equipe para manter todas as partes interessadas informadas e alinhadas com as melhores práticas.

- Gerenciamento de documentação. Mantenha a documentação atual e controlada por versão dos procedimentos de WorkSpaces aplicativos em um local central para garantir a consistência operacional e o compartilhamento de conhecimento entre as equipes.
- Documentação necessária: mantenha a up-to-date documentação para operações críticas de WorkSpaces aplicativos para criação e gerenciamento de imagens, operações de frota e solução de problemas.
- Revisões operacionais: monitore e analise os principais aspectos operacionais, incluindo métricas de desempenho e gerenciamento de incidentes.

- Melhoria contínua. Melhore sistematicamente as operações dos WorkSpaces aplicativos incorporando AWS service (Serviço da AWS) atualizações, métricas operacionais e melhores práticas aprendidas em procedimentos padrão.
 - Atualizações de serviço: monitore as notas de lançamento do WorkSpaces Applications para ver novos recursos, aprimoramentos de serviços, atualizações de segurança e disponibilidade regional.
 - Melhores práticas: revise e incorpore atualizações do AWS Well-Architected Framework WorkSpaces , melhores práticas AWS de aplicativos, arquiteturas de referência e recomendações de segurança. AWS
 - Gerenciamento do conhecimento: mantenha e atualize procedimentos operacionais padrão, runbooks, guias de solução de problemas e documentação de suporte ao usuário.

Antecipe a falha

Realize testes de cenários de falha regularmente para entender os riscos, validar os procedimentos de resposta e melhorar a prontidão da equipe para lidar com incidentes reais.

- Teste de falha. Simule e teste regularmente falhas, como esgotamento da capacidade da frota, falhas no lançamento de aplicativos e problemas de conectividade de rede.
 - Esgotamento da capacidade da frota:
 - Monitore e teste o comportamento de escalabilidade da frota ao se aproximar dos limites de capacidade.
 - Configure CloudWatch alarmes `CapacityUtilization` e `AvailableCapacity` métricas.
 - Implemente procedimentos para lidar com restrições de capacidade durante o pico de uso.
 - Falhas na inicialização do aplicativo:
 - Teste o comportamento de lançamento de aplicativos em instâncias de streaming.
 - Valide o acesso e o desempenho dos aplicativos em diferentes configurações de frota.
 - Problemas de conectividade de rede:
 - Teste o desempenho da sessão de streaming em diferentes condições de rede.
 - Monitore `StreamingSessionLatency` os problemas de qualidade da conexão.
 - Garanta a configuração adequada das configurações da VPC e dos grupos de segurança.
- Procedimentos de recuperação. Desenvolva e teste procedimentos para:

- Failover de frota entre Zonas de disponibilidade da AWS. Além disso, documente procedimentos para escalar a capacidade da frota, gerenciar atualizações da frota e responder aos problemas de saúde da instância.
- Gerenciamento de dados do usuário:
 - Configure e teste as soluções de [persistência e armazenamento de configurações de aplicativos](#) para pastas iniciais no Amazon Simple Storage Service (Amazon S3) para frotas Windows e sistemas de arquivos compartilhados no Amazon Elastic File System (Amazon EFS) para frotas Linux.
 - Valide a sincronização de dados entre as sessões.
- Continuidade do serviço. Mantenha procedimentos para criar novas instâncias de frota, gerenciar atualizações de imagens e lidar com desconexões de sessões.
- Gerenciamento de riscos. Identifique e mitigue:
 - Restrições de capacidade, definindo a capacidade mínima apropriada da frota, configurando políticas de escalabilidade automática com base nos padrões de demanda e monitorando as tendências de utilização da frota usando CloudWatch métricas como, e. `CapacityUtilization` `InUseCapacity` `AvailableCapacity`
 - Gargalos de desempenho rastreando as principais métricas, como `StreamingSessionLatency` e configurando os alarmes apropriados. CloudWatch

Aprenda com todos os eventos e métricas operacionais

Promova uma cultura de melhoria contínua compartilhando lições aprendidas com eventos operacionais e falhas em toda a organização. Enfatize seu impacto nos resultados comerciais.

- Análise de eventos. Documente e analise as interrupções do serviço, a degradação do desempenho, as reclamações dos usuários e os problemas de capacidade.
- Revisão de métricas. Analise padrões de uso, tendências de desempenho, métricas de custo e dados de satisfação do usuário regularmente.
- Compartilhamento de conhecimento. Estabeleça processos para sessões de aprendizado em equipe, documentação de melhores práticas, transferência de conhecimento entre equipes e retrospectivas de incidentes.

Use serviços gerenciados

Minimize a sobrecarga operacional usando serviços AWS gerenciados e criando procedimentos padronizados em torno deles. Integre com os seguintes serviços AWS gerenciados:

- [AWS Systems Manager](#) para automação
- [Amazon CloudWatch](#) para monitoramento
- [AWS Identity and Access Management \(IAM\)](#) para controle de acesso
- [Amazon S3](#) para armazenamento de usuários para frotas Windows
- [Amazon EFS](#) para armazenamento de usuários para frotas Linux
- [AWS Directory Service](#) para autenticação do usuário

Pilar Segurança

O [Pilar de segurança](#) do AWS Well-Architected Framework se concentra em aproveitar os recursos da nuvem para ajudar a estabelecer mecanismos de proteção robustos para suas informações, infraestrutura e recursos. Esses princípios ajudam a aprimorar sua postura geral de segurança e, ao mesmo tempo, possibilitam a inovação.

Principais áreas de foco para aplicar esse pilar ao seu ambiente de streaming de WorkSpaces aplicativos:

- Integridade e confidencialidade dos dados
- Gerenciamento de permissões de usuário
- Estabelecendo controles para detectar eventos de segurança

Implemente uma base sólida de identidade

Use as permissões mínimas necessárias para acessar AWS recursos enquanto centraliza o gerenciamento de identidades e evita credenciais de longo prazo.

- Conceda permissões menos privilegiadas para recursos de WorkSpaces aplicativos:
 - Crie funções específicas do IAM para frotas de WorkSpaces aplicativos com o mínimo de permissões necessárias.
 - Configure permissões limitadas do IAM para criadores de imagens.
 - Restrinja o acesso administrativo às funções de gerenciamento de WorkSpaces aplicativos.
 - Defina permissões granulares para gerenciamento de pilhas e frotas.
- Implemente mecanismos adequados de autenticação do usuário:
 - Configure a federação SAML 2.0 para integração de provedores de identidade corporativa.
 - Configurado [AWS IAM Identity Center](#) para gerenciamento de usuários.
 - Use agentes de identidade personalizados somente quando necessário para cenários de autenticação específicos.
 - Implemente a autenticação multifatorial (MFA) quando houver suporte.
- Controle o acesso do usuário aos aplicativos:
 - Configure os direitos do aplicativo para restringir o acesso a aplicativos específicos.

- Crie grupos de atribuição de aplicativos com base nas funções do usuário.
- Gerencie o acesso ao aplicativo por meio de permissões de pilha.
- Implemente políticas de sessão para controlar o comportamento do aplicativo.
- Proteja as sessões do usuário com os controles apropriados:
 - Configure as políticas de tempo limite da sessão.
 - Defina ações de tempo limite de desconexão.
 - Implemente os requisitos de persistência da sessão.
 - Controle as permissões de redirecionamento do sistema de arquivos.
- Configure a autenticação baseada em certificado para aplicativos. WorkSpaces Para obter mais informações, consulte a postagem do AWS blog [Simplifique a autenticação baseada em certificados para WorkSpaces aplicativos e WorkSpaces com o CA privada da AWS Connector for Active Directory](#).
- Use tags de sessão para implementar um controle de acesso refinado. Para obter mais informações, consulte a postagem do AWS blog [Use tags de sessão para simplificar as permissões WorkSpaces dos aplicativos](#).

Mantenha a rastreabilidade

Implemente monitoramento em tempo real e sistemas de resposta automatizados para todas as mudanças e atividades do ambiente.

- Configure o [CloudWatch registro](#) de registros de aplicativos para monitorar eventos específicos do aplicativo, incluindo inicializações, falhas e erros do aplicativo. Configure os registros da sessão para rastrear as informações da sessão de streaming, incluindo inícios e paradas da sessão e eventos de conexão do usuário.
- [Ative CloudTrail para registrar todas as chamadas da API de WorkSpaces aplicativos](#) e rastrear eventos de gerenciamento, como criação e modificações de frotas, operações de criação de imagens, configurações de pilha e atividades de gerenciamento de usuários.
- Monitore a atividade da instância de WorkSpaces aplicativos:
 - Configure o registro de instâncias para capturar eventos no nível do sistema.
 - Rastreie lançamentos e falhas de aplicativos.
 - Monitore o uso e o desempenho dos recursos do sistema.
- Rastreie a atividade do usuário:

- Monitore as tentativas e falhas de autenticação do usuário. Use CloudWatch métricas e CloudWatch registros para monitorar as tentativas de login do usuário, os horários de início e término da sessão e os eventos de desconexão da sessão.
- Acompanhe os padrões de uso do aplicativo. [Ative os relatórios de uso de WorkSpaces aplicativos](#) para recuperar informações como duração da sessão, horários de início e término, tipos de instância usados e aplicativos acessados.
- Registre as atividades do sistema de arquivos por meio de pastas pessoais habilitadas.
- Defina as configurações da área de transferência e as operações de impressão para atingir suas metas de prevenção de perda de dados.
- Configure [CloudWatch alarmes](#) para métricas relacionadas à segurança, como falhas na autenticação do usuário, padrões de sessão incomuns e violações de acesso a recursos.
- Use o kit de ferramentas EUC para rastrear sessões e estados ativos, monitorar endereços IP para sessões ativas em uso e exportar dados da sessão para auditoria. Para obter mais informações, consulte a postagem do AWS blog [Use o kit de ferramentas EUC para gerenciar os WorkSpaces aplicativos da Amazon e a Amazon](#). WorkSpaces

Aplique segurança em todas as camadas

Implemente várias camadas de controles de segurança em todos os componentes da sua infraestrutura, da borda da rede ao código do aplicativo.

- Configure a segurança da camada de rede:
 - Implemente regras rígidas de grupos de segurança.
 - Coloque WorkSpaces as instâncias da frota de aplicativos em sub-redes privadas que não têm acesso direto à Internet. Controle o acesso à Internet por meio de dispositivos NAT.
 - Use endpoints de nuvem privada virtual (VPC) para acessar os compatíveis Serviços da AWS (como o Amazon S3).
 - Implemente listas de controle de acesso à rede (ACLs) como uma camada adicional de segurança de rede.
 - Restrinja o acesso à porta de streaming (TCP 8443 para HTTPS e WebSocket seguro) a intervalos de IP específicos.
- Configure a segurança da camada de acesso:

- Implemente políticas de tempo limite de sessão para desconectar automaticamente usuários inativos.
- Implemente o controle de acesso baseado em atributos usando tags de sessão. Para obter mais informações, consulte a postagem do AWS blog [Use tags de sessão para simplificar as permissões WorkSpaces dos aplicativos](#).
- Configure a segurança da camada de aplicativo:
 - Configure os direitos do aplicativo para controlar quais usuários podem acessar aplicativos específicos.
 - Ative os controles de redirecionamento do sistema de arquivos para restringir o acesso às unidades locais.
 - Configure as permissões de prancheta, transferência de arquivos e impressão com base nos requisitos de segurança.
 - Configure os controles de acesso ao dispositivo USB de acordo com as políticas de segurança.
- Configure a segurança da camada de imagem:
 - Crie e mantenha imagens básicas reforçadas que atendam aos requisitos de segurança.
 - Mantenha as imagens básicas atualizadas com os patches de segurança mais recentes.
 - Defina as configurações de segurança do Windows nas imagens básicas.
 - Desative serviços e recursos desnecessários do Windows nas imagens básicas.

Automatize as melhores práticas de segurança

Use controles de segurança automatizados e definidos por código em modelos com controle de versão para permitir a implantação segura e escalável da infraestrutura.

- Use a infraestrutura como código (IaC) usando serviços como AWS CloudFormation implementar configurações de segurança consistentes em todas as implantações da frota. Para obter mais informações, consulte a postagem do AWS blog [Anexar automaticamente grupos de segurança adicionais à Amazon WorkSpaces Applications e à Amazon WorkSpaces](#).
- Automatize os processos de segurança de criação de imagens usando a CLI do Image Assistant.
- Configure respostas automatizadas para limites de utilização de capacidade excedidos, tentativas de acesso não autorizado e alterações no grupo de segurança usando alarmes da Amazon CloudWatch, EventBridge regras e AWS Lambda funções da Amazon para respostas automatizadas.

Mantenha as pessoas longe dos dados

Automatize os processos de tratamento de dados para minimizar o acesso humano direto e reduzir o risco de erros ou manuseio incorreto.

- Configure os direitos do aplicativo para controlar quais usuários podem acessar aplicativos específicos.
- Use a [estrutura dinâmica de aplicativos](#) para criar um provedor de aplicativos dinâmico para disponibilizar aplicativos dinamicamente com base nos atributos do usuário.
- Configure o redirecionamento do sistema de arquivos para controlar quais unidades locais os usuários podem acessar, restringir o acesso a pastas específicas e gerenciar permissões de transferência de arquivos entre sessões locais e de streaming.
- Implemente restrições da área de transferência para desativar o compartilhamento da área de transferência entre sessões locais e de streaming, habilite o fluxo unidirecional da área de transferência quando necessário e evite a cópia não autorizada de dados.
- Defina a persistência das configurações do aplicativo para salvar e restaurar automaticamente as configurações do aplicativo, eliminar as necessidades de configuração manual e manter experiências de usuário consistentes.

Prepare-se para eventos de segurança

Desenvolva e pratique planos de resposta a incidentes usando ferramentas automatizadas para permitir a rápida detecção, investigação e recuperação de eventos de segurança.

- Configure CloudWatch alarmes para tentativas de autenticação malsucedidas, alterações nos grupos de segurança da frota, modificações nas configurações de imagem e padrões incomuns de sessão de streaming.
- Documente os procedimentos de resposta para cenários comuns de segurança de WorkSpaces aplicativos, como:
 - Tentativas de acesso não autorizado
 - Detecção: monitore falhas de autenticação.
 - Resposta: revogue os direitos do usuário, revise os registros da sessão e atualize as políticas de acesso.
 - Instâncias de streaming comprometidas

- Detecção: monitore o comportamento da instância.
- Resposta: encerre as sessões afetadas, substitua as instâncias da frota e revise as configurações do grupo de segurança.
- Tentativas de exfiltração de dados
 - Detecção: monitore as atividades de transferência de arquivos.
 - Resposta: revise os registros da área de transferência e de transferência de arquivos, ajuste as permissões de transferência de arquivos e atualize as políticas de proteção de dados.
- Implemente processos de recuperação automatizados para substituição de instâncias de frota, restauração de grupos de segurança, reconfiguração de acesso de usuários e recuperação de configurações de aplicativos.
- Use Serviços da AWS para gerenciamento de segurança, como AWS Security Hub CSPM para descobertas de segurança e Amazon GuardDuty para detecção de ameaças.

Pilar Confiabilidade

O [pilar de confiabilidade](#) do AWS Well-Architected Framework aborda o quão bem um sistema mantém a funcionalidade e os níveis de desempenho pretendidos durante os períodos operacionais esperados ao longo de sua vida útil. Ele fornece diretrizes abrangentes para criar e manter sistemas confiáveis AWS, incluindo estratégias para teste e validação em todos os estágios do ciclo de vida da carga de trabalho.

Principais áreas de foco para aplicar esse pilar ao seu ambiente de streaming de WorkSpaces aplicativos:

- Gerenciamento e escalabilidade da frota
- Confiabilidade da sessão
- Disponibilidade da aplicação
- Procedimentos de recuperação

Recuperação automática de falhas

Monitore o valor comercial KPIs para acionar respostas automatizadas que possam prever, prevenir ou se recuperar de falhas antes que elas afetem as operações.

- Certifique-se de que a alocação de sub-redes IP considere a expansão e a disponibilidade.
- Monitore CloudWatch métricas críticas para garantir a disponibilidade e o desempenho do serviço, incluindo métricas de capacidade da frota, como `AvailableCapacity` e `InUseCapacity`, e métricas de qualidade de streaming, como `StreamingSessionLatency`.
- Configure alertas para limites de capacidade, métricas de integridade da sessão, degradação do desempenho e alterações no status de integridade da frota.
- Use os recursos de escalabilidade automática de WorkSpaces aplicativos integrados para:
 - Configure a capacidade mínima e máxima da frota.
 - Defina políticas de escalabilidade com base na utilização da capacidade.
 - Defina limites de expansão e retração com base nas métricas de experiência do usuário e nos requisitos de negócios, em vez de apenas métricas técnicas.

- Crie um ambiente de recuperação de desastres para seu ambiente de WorkSpaces aplicativos. Para obter mais informações, consulte a postagem do AWS blog [Considerações sobre recuperação de desastres com WorkSpaces aplicativos da Amazon](#).

Testar os procedimentos de recuperação

Os ambientes em nuvem permitem testes automatizados de cenários de falha e procedimentos de recuperação. Esses recursos ajudam você a identificar e corrigir vulnerabilidades antes que ocorram falhas reais.

- Teste de recuperação de frota. Implemente testes abrangentes de recuperação de frota em vários cenários:
 - Simule o encerramento da instância para verificar a resposta automática do escalonamento.
 - Valide a manutenção da capacidade mínima da frota.
 - Tempo de substituição da instância de teste e redirecionamento do usuário.
 - Valide a eficácia das políticas de escalabilidade.
 - Teste os limites de capacidade da frota e o tratamento de transbordamento.
- Teste de recuperação de sessão. Implemente procedimentos de validação de recuperação de sessão:
 - Teste cenários de desconexão e reconexão.
 - Verifique a preservação do estado do aplicativo.
 - Teste vários cenários de interrupção da rede.
 - Valide os comportamentos de tempo limite da sessão.
 - Verifique a persistência da autenticação do usuário.
 - Verifique o manuseio do armazenamento temporário.

Dimensione horizontalmente para aumentar a disponibilidade da carga de trabalho agregada

Distribua sua carga de trabalho em vários recursos menores para minimizar o impacto de falhas individuais e eliminar pontos únicos de falha.

- Implante instâncias de frota em várias zonas de disponibilidade.

- Configure a capacidade mínima apropriada da frota.
- Configure o escalonamento automático para frotas e defina os limites de escalabilidade apropriados.
- Monitore a utilização da capacidade em toda a frota.
- Implante pilhas de WorkSpaces aplicativos em várias regiões. Para obter mais informações, consulte a postagem do AWS blog [Otimize a experiência do usuário com roteamento baseado em latência para aplicativos da Amazon WorkSpaces](#)

Pare de adivinhar a capacidade

Use os recursos de escalabilidade automática da nuvem para ajustar dinamicamente os recursos com base na demanda. Isso ajuda a evitar a saturação de recursos enquanto mantém a eficiência ideal.

- Monitore as principais métricas `CapacityUtilization`, como `AvailableCapacity`, e `InUseCapacity` para entender as necessidades de capacidade.
- Acompanhe as tendências de utilização da frota em diferentes períodos de tempo. Monitore padrões diários, variações semanais, tendências mensais e picos sazonais.
- Configure políticas de escalabilidade e configure limites de escalabilidade.
- Certifique-se de que existe uma lacuna suficiente entre as cotas atuais e o uso máximo para acomodar o failover.
- Projete cotas e restrições de serviço fixas por meio da sua arquitetura.

Gerencie mudanças por meio da automação

Implemente mudanças na infraestrutura por meio da automação, incluindo alterações controladas por versão no próprio código de automação.

- Use o IaC para configuração da frota.
- Implemente políticas de escalabilidade consistentes.
- Use a [CLI do Image Assistant para criar](#) imagens de forma consistente.

Pilar Eficiência de performance

O [pilar de eficiência de desempenho](#) do AWS Well-Architected Framework se concentra na otimização do uso dos recursos da nuvem para atender ou superar as metas de desempenho, garantindo a adaptabilidade às demandas flutuantes e às tecnologias emergentes. Ele enfatiza a importância de ajustar continuamente os sistemas para manter a máxima eficiência em um ambiente dinâmico de nuvem.

Principais áreas de foco para aplicar esse pilar ao seu ambiente de streaming de WorkSpaces aplicativos:

- Seleção e otimização do tipo de instância
- Otimização do desempenho de streaming
- Gerenciamento da capacidade da frota

Democratize tecnologias avançadas

Aproveite os serviços de nuvem gerenciados pelo fornecedor para tecnologias complexas para que sua equipe possa se concentrar no desenvolvimento de produtos em vez do gerenciamento da infraestrutura.

- Configure os tipos de instância apropriados com base nos requisitos do aplicativo:
 - Selecione instâncias habilitadas para GPU para aplicativos com uso intenso de gráficos.
 - Escolha [as famílias de GPU](#) apropriadas (como Graphics G4dn ou Graphics G5) com base nas necessidades do aplicativo.
- Escolha e configure um dos seguintes métodos de autenticação:
 - Configure a integração com um provedor de identidade baseado em SAML 2.0.
 - Defina as configurações do grupo de usuários.
 - Integre com [AWS Directory Service](#).
- Ative e configure as opções de armazenamento com base nas necessidades do usuário:
 - Configure pastas pessoais no [Amazon S3](#) para frotas baseadas em Windows.
 - Configure sistemas de arquivos compartilhados no [Amazon EFS](#) para frotas baseadas em Linux.
 - Configure permissões de armazenamento persistentes.
 - Ative a persistência das configurações do aplicativo.

Torne-se global em minutos

Use a implantação em várias regiões para melhorar as experiências globais do usuário por meio da redução da latência.

- Configure frotas em várias Regiões da AWS implantando frotas nas regiões mais próximas de seus usuários e criando pilhas separadas para cada região.
- Implemente o redirecionamento entre regiões para redirecionar automaticamente os usuários dos WorkSpaces aplicativos para as AppStream pilhas que estão mais próximas de sua localização atual.
- Se você estiver usando qualquer um dos recursos opcionais em WorkSpaces Aplicativos, como persistência de configurações de aplicativos, pastas iniciais ou frotas elásticas, precisará configurar a replicação entre regiões do Amazon S3 para dados do usuário para frotas baseadas em Windows e a replicação entre regiões para frotas baseadas em Linux.
- Replique imagens em todas as regiões. Para obter mais informações, consulte [Copiar uma imagem que você possui para outra Região da AWS no Amazon WorkSpaces Applications](#) na AWS documentação.
- Para frotas unidas ao domínio, certifique-se de que uma infraestrutura do Active Directory, incluindo os Serviços de Federação do Active Directory (AD FS) (a menos que você esteja usando o SAML 2.0 e o Amazon Cognito como alternativa), esteja configurada adequadamente nas outras regiões e que você use para recursos de replicação em várias regiões. [AWS Directory Service for Microsoft Active Directory](#)
- Direcione os usuários para os endpoints de aplicativos de menor latência. WorkSpaces Para obter mais informações, consulte a postagem do AWS blog [Otimize a experiência do usuário com roteamento baseado em latência para](#) aplicativos da Amazon. WorkSpaces

Use arquiteturas sem servidor

As arquiteturas sem servidor eliminam a sobrecarga de gerenciamento do servidor e reduzem os custos usando serviços gerenciados em nuvem para funções de computação.

Use serviços AWS sem servidor, como os seguintes:

- [AWS Lambda](#) para automatizar tarefas e integrar lógica personalizada por meio de funções orientadas por eventos

- [Amazon S3](#) fornecerá armazenamento escalável para aplicativos, dados de usuários, arquivos de WorkSpaces aplicativos e artefatos de sessão
- [A Amazon CloudWatch](#) fornecerá monitoramento, registro e alertas para métricas de desempenho e uso de WorkSpaces aplicativos
- [Amazon Cognito para](#) facilitar a autenticação de usuários e o controle de acesso para aplicativos WorkSpaces
- [Amazon API Gateway](#) RESTful APIs para criar uma interface entre WorkSpaces aplicativos e outros serviços ou aplicativos personalizados

Experimente com mais frequência

A infraestrutura em nuvem permite testes rápidos de várias configurações de recursos para otimizar o desempenho e o custo.

- Teste diferentes tipos de instância para otimizar o desempenho e o custo:
 - Compare o desempenho do stream em diferentes famílias de instâncias.
 - Avalie instâncias de GPU versus instâncias sem GPU para aplicativos gráficos.
 - Teste instâncias otimizadas para memória para aplicativos que consomem muita memória.
- Teste as configurações do aplicativo usando o Image Builder:
 - Crie imagens de teste com diferentes configurações de aplicativos.
 - Valide o desempenho do aplicativo antes da implantação.
 - Teste a compatibilidade do aplicativo com diferentes tipos de instância.
- Teste as configurações da frota usando configurações de capacidade da frota, como capacidade mínima e máxima, políticas de escalabilidade, configurações de sessão, como duração máxima da sessão, e configurações de tempo limite de desconexão.

Considere a simpatia mecânica

Escolha serviços em nuvem com base nos requisitos e padrões de uso específicos de sua carga de trabalho para garantir desempenho e eficiência ideais.

- Escolha instâncias Graphics G5 para aplicativos com uso intensivo de gráficos, aplicativos que exigem software de visualização DirectX, OpenGL, OpenCL ou 3D.

- Selecione `stream.standard` instâncias para aplicativos de negócios, navegadores da web e aplicativos gráficos leves
- Monitore e ajuste o protocolo de streaming com base em CloudWatch métricas como `StreamingSessionLatency`.
- Configure VPCs os WorkSpaces aplicativos mais próximos de seus usuários e use a largura de banda de rede adequada com base nos requisitos do seu aplicativo.
- Escolha o tipo de frota adequado com base no comportamento do aplicativo. Por exemplo, escolha frotas de sessão única para aplicativos que exigem recursos dedicados e frotas de várias sessões para aplicativos que podem compartilhar recursos de forma eficiente.
- Considere a compatibilidade de aplicativos com ambientes de várias sessões.
- Use o [recurso de redirecionamento do sistema de arquivos](#) para lidar com as interações entre aplicativos remotos e locais. Para obter mais informações, consulte a postagem do AWS blog [Lançamento de aplicativos locais a partir de uma sessão de streaming do Amazon WorkSpaces Applications](#).

Pilar Otimização de custos

O [pilar de otimização de custos](#) do AWS Well-Architected Framework se concentra em maximizar o valor comercial e minimizar as despesas. Isso ajuda a garantir que cada dólar gasto em recursos de nuvem contribua de forma eficaz para alcançar seus objetivos organizacionais.

Principais áreas de foco para aplicar esse pilar ao seu ambiente de streaming de WorkSpaces aplicativos:

- Gerenciamento da capacidade da frota e seleção do tipo de instância
- Otimização de escalonamento e agendamento
- Monitoramento e análise de padrões de uso
- Alocação e rastreamento de custos

Implementar o gerenciamento financeiro da nuvem

Crie capacidade organizacional dedicada em gerenciamento financeiro e otimização de custos na nuvem por meio de programas e processos estruturados para maximizar o valor e a eficiência da nuvem.

- Monitore os custos dos WorkSpaces aplicativos usando relatórios de uso [AWS Cost Explorer](#) e uso para rastrear o uso das horas de streaming, analisar os custos das instâncias da frota e monitorar a distribuição regional de custos.
- Planeje e defina controles de custo usando [AWS Budgets](#) para definir alertas para os custos gerais do serviço de WorkSpaces aplicativos, criar limites orçamentários para o serviço e monitorar os gastos reais em relação aos valores orçados. Para obter mais informações, consulte a postagem do AWS blog [Como usar a automação para otimizar e controlar os custos dos WorkSpaces aplicativos da Amazon](#).

Adicionar um modelo de consumo

Dimensione os recursos e os custos de computação com base nos padrões reais de uso. Por exemplo, você pode desligar ambientes que não sejam de produção fora do horário comercial para otimizar os gastos.

- Escolha o modelo de preços adequado. Por exemplo, use frotas sempre ativas para uso consistente e frotas sob demanda para cargas de trabalho variáveis.
- Selecione os tipos de instância ideais. Por exemplo, use `stream.standard` instâncias para aplicativos gerais e use instâncias gráficas (G4dn) somente quando necessário.

Meça a eficiência geral

Calcule e acompanhe cost-per-unit a produção comercial para quantificar as melhorias de eficiência e orientar os esforços de otimização.

- Monitore a eficiência da sessão.
- Monitore a utilização da frota usando as seguintes CloudWatch métricas:
 - `AvailableCapacity` para rastrear a capacidade não utilizada
 - `InUseCapacity` para medir o uso real
- Calcule e acompanhe os custos por sessão, como custo por hora de streaming, custo por usuário e custo por aplicativo.
- Implemente o [Cost Optimizer for WorkSpaces Applications](#) para monitorar seus construtores.
- Compare os custos entre os tipos de frota. Por exemplo, compare:
 - Custos de licença para sessões únicas e várias sessões
 - Taxas de utilização de recursos
 - Densidade de usuários por instância
- Use dados de rastreamento de processos para identificar aplicativos subutilizados ou desnecessários. Para obter mais informações, consulte a postagem do AWS blog [Rastreie os processos do usuário nas sessões do Amazon WorkSpaces Applications](#).

Pare de gastar dinheiro em levantamento de peso indiferenciado

AWS gerencia as operações de infraestrutura e oferece serviços gerenciados para que sua organização possa se concentrar nos objetivos de negócios em vez da manutenção de TI.

- Crie e mantenha imagens de aplicativos usando o Image Builder para empacotar seus aplicativos, definir as configurações do aplicativo e testar a compatibilidade do aplicativo.
- Configure as especificações da frota selecionando os tipos de instância apropriados, definindo limites de escalabilidade e definindo os limites de capacidade desejados.

- [Configure opções de armazenamento persistente configurando pastas iniciais no Amazon S3 para frotas baseadas em Windows e sistemas de arquivos compartilhados no Amazon EFS para frotas baseadas em Linux.](#) Defina permissões de armazenamento e defina políticas de retenção.

Analise e atribua despesas

A nuvem permite o rastreamento preciso do uso de recursos e dos custos por carga de trabalho, o que permite medições precisas de retorno sobre o investimento (ROI) e oportunidades de otimização direcionadas.

- Implemente uma estratégia abrangente de marcação para frotas para alocação de custos, imagens para rastreamento de ativos, criadores de imagens para designação de ambientes e pilhas para agrupamento organizacional.
- Use os [Relatórios de AWSAWS Custo e Uso \(CUR\)](#) para detalhar os custos dos WorkSpaces aplicativos por recursos marcados e analisar os custos por frota, pilha e imagem.
- Use [AWS Cost Explorer](#) para visualizar tendências de gastos com WorkSpaces aplicativos e comparar custos em diferentes dimensões, como regiões e tipos de instância.
- Monitore e analise as taxas de utilização da frota, a eficiência do tipo de instância e as horas de streaming por aplicativo.
- Rastreie a capacidade reservada não utilizada, frotas ou pilhas subutilizadas e os períodos de inatividade no uso da frota.
- Calcule e acompanhe o custo por usuário para cada aplicativo, as horas de streaming por aplicativo e as taxas de adoção de usuários para aplicativos transmitidos.
- Configure uma análise de uso detalhada configurando relatórios de uso de WorkSpaces aplicativos, usando o [Amazon Athena](#) para consultar dados de uso e criando visualizações [no Amazon Quick](#) para obter insights de custo e uso.
- Avalie as considerações de custo total, como licenciamento do Windows Server, modelos de licenciamento de aplicativos e licenciamento por usuário, em comparação com o licenciamento por dispositivo.
- Use o Amazon Athena para consultar e analisar os custos de armazenamento da pasta inicial e os padrões de uso por usuário. Para obter mais informações, consulte a postagem do AWS blog [Como relatar o uso da pasta inicial do Amazon WorkSpaces Applications com o Amazon Athena.](#)

Pilar Sustentabilidade

O [pilar de sustentabilidade](#) do AWS Well-Architected Framework enfatiza a minimização de sua pegada ambiental e a otimização do uso e da eficiência de energia. Ele orienta os arquitetos a tomarem decisões ambientalmente conscientes em seus projetos de sistemas e estratégias de alocação de recursos.

Principais áreas de foco para aplicar esse pilar ao seu ambiente de streaming de WorkSpaces aplicativos:

- Compreender e otimizar a alocação de recursos para atender à demanda real e minimizar o desperdício em ambientes de streaming
- Análise e adaptação aos padrões de consumo do usuário para melhorar a eficiência da entrega de aplicativos e das sessões de streaming
- Selecionar e usar configurações de hardware apropriadas para maximizar a eficiência energética e, ao mesmo tempo, atender aos requisitos de desempenho
- Usando recursos de serviços AWS gerenciados para se beneficiar das economias de escala e dos recursos de eficiência integrados oferecidos por esses serviços

Análise do seu impacto

Monitore e otimize o impacto ambiental de sua carga de trabalho medindo a eficiência dos recursos e as emissões por unidade de produção. Use esses dados para estabelecer KPIs e orientar melhorias na sustentabilidade.

- Monitore os padrões de utilização da frota.
- Acompanhe as horas de streaming por usuário.
- Analise as tendências de uso da capacidade da frota.

Estabeleça metas de sustentabilidade

Defina metas de sustentabilidade mensuráveis para cada carga de trabalho que se alinhem aos objetivos organizacionais. Concentre-se em reduzir a intensidade de recursos por transação à medida que você cresce.

- Defina metas para taxas de utilização da frota, eficiência do tipo de instância e otimização das horas de streaming.
- Planeje a capacidade com base nos padrões reais de uso.

Maximize a utilização

Otimize a eficiência da carga de trabalho dimensionando corretamente os recursos e maximizando a utilização. Reduza a capacidade ociosa para minimizar o consumo de energia e melhorar a sustentabilidade.

- Configure o escalonamento automático para atender à demanda real.
- Capacidade de frota do tamanho certo com base nos padrões de uso.
- Implemente limites de capacidade mínima e máxima apropriados.
- Escolha os tipos de instância apropriados para cargas de trabalho.
- Monitore e otimize a densidade da sessão de streaming.
- Reduza a capacidade ociosa fora dos horários de pico.

Antecipe e adote ofertas de hardware e software novas e mais eficientes

Mantenha-se informado e adote rapidamente novas tecnologias eficientes de parceiros e fornecedores para melhorar continuamente o impacto ambiental de sua carga de trabalho.

- Use os tipos de instância da geração atual.
- Atualize para tipos de instância mais novos quando disponíveis.
- Otimize as configurações de streaming do aplicativo.
- Configure os protocolos de streaming apropriados.
- Atualize para os recursos mais recentes WorkSpaces dos aplicativos.

Serviços gerenciados usados

Aproveite os serviços de nuvem compartilhada e as soluções gerenciadas para maximizar a eficiência da utilização de recursos e, ao mesmo tempo, minimizar o impacto ambiental por meio do dimensionamento automatizado e do gerenciamento do ciclo de vida.

- Use o [Amazon S3](#) para armazenamento de usuários para frotas baseadas em Windows e o [Amazon EFS](#) para sistemas de arquivos compartilhados para frotas baseadas em Linux.
- Implemente [CloudWatch](#) para monitoramento.
- Configure o [IAM](#) para gerenciamento de acesso.

Reduza o impacto posterior de suas cargas de trabalho na nuvem

Serviços de design para minimizar os requisitos de recursos do lado do cliente, reduzir o consumo de energia e prolongar a vida útil dos dispositivos para os usuários.

- Ajuste a duração máxima da sessão para evitar o consumo desnecessário de recursos.
- Configure os tempos limite de sessão apropriados.
- Defina políticas de tempo limite de desconexão.
- Implemente políticas de persistência da sessão quando necessário.

Recursos

AWS documentação

- [AWS Well-Architected Framework](#)
- [Guia de administração WorkSpaces de aplicativos da Amazon](#)
- [Guia CloudWatch do usuário da Amazon](#)
- [Guia do usuário do Amazon EFSS](#)
- [Guia do usuário do Amazon S3](#)
- [Guia do usuário do IAM](#)

AWS postagens no blog

- [WorkSpaces Aplicativos baseados em associação a grupos do Active Directory e segmentação de aplicativos](#)
- [Crie um único provedor de identidade para todas as suas pilhas de WorkSpaces aplicativos da Amazon com o Azure AD](#)
- [Configurando a assistência remota do Windows para a Amazon WorkSpaces e os aplicativos da Amazon WorkSpaces](#)
- [Criação de um registro AS2 TrustedDomains DNS TXT para redirecionar o cliente nativo do Amazon WorkSpaces Applications para um provedor de identidade terceirizado](#)
- [Criação de registros personalizados e CloudWatch alertas da Amazon nos aplicativos da Amazon WorkSpaces](#)
- [Redirecionamento entre regiões com Geo Targetly e Amazon Applications WorkSpaces](#)
- [Recursos entre contas e aplicativos da Amazon WorkSpaces](#)
- [Habilite a federação com Bio-key e PortalGuard Amazon Applications WorkSpaces](#)
- [Habilitando a federação com WorkSpaces aplicativos Simple SAMLphp e Amazon](#)
- [Habilitando a federação de identidades com Duo Single Sign-On e Amazon Applications WorkSpaces](#)
- [Habilitando a federação de identidades com aplicativos Shibboleth e Amazon WorkSpaces](#)
- [Estratégias de failover para VDI local com Amazon End User Computing](#)

- [Como a Amazon usa os WorkSpaces aplicativos da Amazon para fornecer aos cientistas e analistas de dados acesso a dados confidenciais](#)
- [Como configurar a autenticação baseada em certificado para aplicativos da Amazon WorkSpaces](#)
- [Como usar reivindicações Okta com direitos de inscrição para aplicativos da Amazon WorkSpaces](#)
- [Gerenciando laboratórios de computação em WorkSpaces aplicativos da Amazon com gerenciamento de aplicativos virtuais de código aberto](#)
- [Métodos de alocação de seus custos de WorkSpaces aplicativos para suas unidades de negócios](#)
- [Monitoramento de WorkSpaces aplicativos da Amazon com o Amazon OpenSearch Service e o Amazon Kinesis Data Firehose](#)
- [Separação de rede e higienização de dados usando Amazon, Amazon WorkSpaces Applications e WorkSpaces Amazon Macie](#)
- [OneLogin SSO com aplicativos da Amazon WorkSpaces](#)
- [Otimize seu caminho de áudio de chamadas do Amazon Connect com os WorkSpaces aplicativos da Amazon](#)
- [Armazenamento persistente para frotas Linux da Amazon WorkSpaces Applications no Amazon Elastic File System](#)
- [Redirecione um aplicativo Okta SAML para o cliente nativo do Amazon WorkSpaces Applications](#)
- [Simplifique o gerenciamento de imagens WorkSpaces dos aplicativos da Amazon com o mascaramento de aplicativos](#)
- [Transmita aplicativos a um custo menor com Amazon WorkSpaces Applications, frotas elásticas e compatibilidade com Linux](#)
- [Streaming a partir de endpoints VPC de interface para ambientes regulamentados com aplicativos WorkSpaces](#)
- [Use os direitos do aplicativo Amazon WorkSpaces Applications com o Azure AD](#)
- [Relator de problemas de usuário para aplicativos da Amazon WorkSpaces](#)
- [Usando os direitos do aplicativo Amazon WorkSpaces Applications com o Google Workspace](#)
- [Usando Auth0 com o Microsoft Active Directory em aplicativos da Amazon WorkSpaces](#)
- [Usando AppLocker a Microsoft para gerenciar a experiência de aplicativos na Amazon WorkSpaces Applications](#)
- [Usando Python para alimentar uma GUI do WorkSpaces Applications Linux Imaging Assistant](#)
- [Opções de redirecionamento de aplicativos Web para o cliente de WorkSpaces aplicativos](#)

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um [feed RSS](#).

Alteração	Descrição	Data
Publicação inicial	—	23 de julho de 2025

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Aurora Edição Compatível com PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape)]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Relational Database Service (Amazon RDS) para Oracle na Nuvem AWS.
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migrar seu sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: migrar seu banco de dados Oracle on-premises para o Oracle em uma instância do EC2 na Nuvem AWS.
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma on-premises para um serviço de nuvem para a mesma plataforma. Exemplo: migrar um Microsoft Hyper-V aplicativo para o AWS
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um

momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.

- Retirar: desative ou remova aplicações que não são mais necessárias em seu ambiente de origem.

A

ABAC

Consulte [controle de acesso baseado em atributo](#).

serviços abstraídos

Veja [serviços gerenciados](#).

ACID

Veja [atomicidade, consistência, isolamento, durabilidade](#).

migração ativa-ativa

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

migração ativa-passiva

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

AGGREGATE FUNCTION

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

AI

Veja [inteligência artificial](#).

AIOps

Veja [operações de inteligência artificial](#).

anonimização

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

antipadrões

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

controle de aplicações

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

O processo de usar técnicas de machine learning para resolver problemas operacionais, reduzir incidentes operacionais e intervenção humana e aumentar a qualidade do serviço. Para obter mais informações sobre como AIOps é usado na estratégia de AWS migração, consulte o [guia de integração de operações](#).

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade (ACID)

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

controle de acesso por atributo (ABAC)

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

fonte de dados autorizada

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

Zona de disponibilidade

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o [site da AWS CAF](#) e o [whitepaper da AWS CAF](#).

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

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

B

bot malicioso

Um [bot](#) destinado a causar disrupção ou danos a indivíduos ou organizações.

BCP

Veja [planejamento de continuidade de negócios](#)

gráfico de comportamento

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

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também [endianness](#).

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

Uma aplicação de software que executa tarefas automatizadas na internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como crawlers da web que indexam informações na internet. Outros bots, conhecidos como bots maliciosos, têm como objetivo causar interrupção ou danos a indivíduos ou organizações.

botnet

Redes de [bots](#) infectadas por [malware](#) e sob o controle de uma única parte, conhecidas como bot herder ou operador de bots. Os botnets são o mecanismo mais conhecido para escalar bots e seu impacto.

ramo

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

Acesso de emergência

Em circunstâncias excepcionais e por meio de um processo aprovado, um meio rápido para um usuário obter acesso a um Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador [Implement break-glass procedures](#) nas orientações do AWS Well-Architected.

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

planejamento de continuidade de negócios (BCP)

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

C

CAF

Veja [AWS Cloud Adoption Framework](#).

implantação canário

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substitui a versão atual por completo.

CCoE

Veja [Centro de Excelência da Nuvem](#).

CDC

Veja [captura de dados de alteração](#).

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja [integração e entrega contínuas](#).

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendadas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as [publicações CCoE](#) no blog de estratégia Nuvem AWS corporativa.

computação em nuvem

A tecnologia de nuvem normalmente usada para armazenamento de dados remoto e gerenciamento de dispositivos de IoT. A computação em nuvem é normalmente conectada à tecnologia de [computação de borda](#).

modelo operacional em nuvem

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

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam ao migrar para a Nuvem AWS:

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

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

CMDB

Veja [banco de dados de gerenciamento de configuração](#).

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

Um campo de [IA](#) que usa machine learning para analisar e extrair informações de formatos visuais, como vídeos e imagens digitais. Por exemplo, a Amazon SageMaker AI fornece algoritmos de processamento de imagem para CV.

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja [visão computacional](#).

D

dados em repouso

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

classificação de dados

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

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

desvio de dados

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

dados em trânsito

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

data mesh

Um framework de arquitetura que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

Um sistema de gerenciamento de dados compatível com business intelligence, como analytics. Os data warehouses geralmente contêm grandes quantidades de dados históricos e geralmente são usados para consultas e análises.

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Veja [linguagem de definição de banco de dados](#).

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta

é chamada de administrador delegado para esse serviço. Para obter mais informações e uma lista de serviços compatíveis, consulte [Serviços que funcionam com o AWS Organizations](#) na documentação do AWS Organizations .

implantação

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

ambiente de desenvolvimento

Veja [ambiente](#).

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Veja [linguagem de manipulação de banco de dados](#).

design orientado por domínio

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

DR

Veja [recuperação de desastres](#).

Deteção da oscilação

Rastreamento de desvios de uma configuração de linha de base. Por exemplo, você pode usar AWS CloudFormation para [detectar desvios nos recursos do sistema](#) ou AWS Control Tower para [detectar mudanças em seu landing zone](#) que possam afetar a conformidade com os requisitos de governança.

DVSM

Veja [mapeamento do fluxo de valor de desenvolvimento](#).

E

EDA

Veja [análise exploratória de dados](#).

EDI

Veja [intercâmbio eletrônico de dados](#).

computação de borda

A tecnologia que aumenta o poder computacional de dispositivos inteligentes nas bordas de uma rede de IoT. Quando comparada com a [computação em nuvem](#), a computação de borda pode reduzir a latência da comunicação e melhorar o tempo de resposta.

intercâmbio eletrônico de dados (EDI)

A troca automatizada de documentos comerciais entre organizações. Para obter mais informações, consulte [O que é EDI \(Intercâmbio eletrônico de dados\)?](#).

criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja [endpoint de serviço](#).

serviço de endpoint

Um serviço que pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros diretores Contas da AWS ou a AWS Identity and Access Management (IAM).

Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais informações, consulte [Criar um serviço de endpoint](#) na documentação do Amazon Virtual Private Cloud (Amazon VPC).

planejamento de recursos empresariais (ERP)

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

criptografia envelopada

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

ambiente

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

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

epic

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

ERP

Veja [planejamento de recursos empresariais](#).

análise exploratória de dados (EDA)

O processo de analisar um conjunto de dados para entender suas principais características. Você coleta ou agrega dados e, em seguida, realiza investigações iniciais para encontrar padrões, detectar anomalias e verificar suposições. O EDA é realizado por meio do cálculo de estatísticas resumidas e da criação de visualizações de dados.

F

tabela de fatos

A tabela central em um [esquema em estrela](#). Ela armazena dados quantitativos sobre as operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: as que contêm medidas e as que contêm uma chave externa para uma tabela de dimensões.

Antecipar-se à falha

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

delimitação de isolamento contra falhas

No Nuvem AWS, um limite, como uma zona de disponibilidade, Região da AWS um plano de controle ou um plano de dados, que limita o efeito de uma falha e ajuda a melhorar a resiliência das cargas de trabalho. Para obter mais informações, consulte [AWS Fault Isolation Boundaries](#).

ramificação de recursos

Veja [ramificação](#).

recursos

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

importância do recurso

O quanto um recurso é importante para as previsões de um modelo. Isso geralmente é expresso como uma pontuação numérica que pode ser calculada por meio de várias técnicas, como

Shapley Additive Explanations (SHAP) e gradientes integrados. Para obter mais informações, consulte [Interpretabilidade do modelo de aprendizado de máquina com AWS](#).

transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo, se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

prompt few shot

Fornecer a um [LLM](#) um pequeno número de exemplos que demonstram a tarefa e o resultado desejado antes de solicitar que ele execute uma tarefa semelhante. Essa técnica é uma aplicação do aprendizado em contexto, em que os modelos aprendem com exemplos (shots) incorporados aos prompts. Prompts few-shot podem ser eficazes para tarefas que exigem formatação, raciocínio ou conhecimento de domínio específicos. Veja também [prompts zero-shot](#).

FGAC

Veja [controle de acesso refinado](#).

Controle de acesso refinado (FGAC)

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

migração flash-cut

Um método de migração de banco de dados que usa replicação contínua de dados via [captura de dados de alteração](#) para migrar os dados no menor tempo possível, em vez de usar uma abordagem em fases. O objetivo é reduzir ao mínimo o tempo de inatividade.

FM

Veja [modelo de base](#).

modelo de base (FM)

Uma grande rede neural de aprendizado profundo que vem treinando em grandes conjuntos de dados generalizados e não rotulados. FMs são capazes de realizar uma ampla variedade de tarefas gerais, como entender a linguagem, gerar texto e imagens e conversar em linguagem natural. Para obter mais informações, consulte [O que são modelos de base?](#).

G

IA generativa

Um subconjunto de modelos de [IA](#) que foram treinados em grandes quantidades de dados e que podem usar um simples prompt de texto para criar novos artefatos e conteúdo, como imagens, vídeos, texto e áudio. Para obter mais informações, consulte [O que é IA generativa?](#).

bloqueio geográfico

Veja [restrições geográficas](#).

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

Uma abordagem na qual ambientes inferiores e superiores usam ramificações diferentes em um repositório de código-fonte. O fluxo de trabalho do Gitflow é considerado legado, e o [fluxo de trabalho trunk-based](#) é a abordagem moderna e preferencial.

golden image

Um snapshot de um sistema ou software usado como modelo para implantar novas instâncias desse sistema ou software. Por exemplo, na manufatura, uma golden image pode ser usada para provisionar software em vários dispositivos e ajudar a melhorar a velocidade, a escalabilidade e a produtividade nas operações de fabricação de dispositivos.

estratégia greenfield

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

barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais (OUs). Barreiras de proteção preventivas impõem políticas para

garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja [alta disponibilidade](#).

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

dados de hold-out

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de [machine learning](#). Você pode usar dados de hold-out para avaliar a performance do modelo comparando as predições do modelo com os dados de retenção.

migração homogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que compartilha o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server para Amazon RDS para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

dados quentes

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

hotfix

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

período de hipercuidados

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

eu

laC

Veja [infraestrutura como código](#).

Política baseada em identidade

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

aplicação ociosa

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

IloT

Veja [Internet das Coisas Industrial](#).

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para workloads de produção em vez de atualizar, aplicar patches ou modificar a infraestrutura existente. Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e preditivas do que [infraestruturas mutáveis](#). Para obter mais informações, consulte a prática recomendada [Implantar usando infraestrutura imutável](#) no AWS Well-Architected Framework.

VPC de entrada (admissão)

Em uma arquitetura de AWS várias contas, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de um aplicativo. A [Arquitetura de Referência de AWS Segurança](#) recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

migração incremental

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

Indústria 4.0

Um termo que foi introduzido por [Klaus Schwab](#) em 2016 para se referir à modernização dos processos de manufatura por meio de avanços em conectividade, dados em tempo real, automação, analytics e IA/ML.

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

O uso de sensores e dispositivos conectados à Internet nos setores industriais, como manufatura, energia, automotivo, saúde, ciências biológicas e agricultura. Para obter mais informações, consulte [Criando uma estratégia de transformação digital industrial da Internet das Coisas \(IIoT\)](#).

VPC de inspeção

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

Internet das coisas (IoT)

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

interpretabilidade

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

IoT

Veja [Internet das Coisas](#).

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Veja [biblioteca de informações de TI](#).

ITSM

Veja [gerenciamento de serviços de TI](#).

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

grande modelo de linguagem (LLM)

Um modelo de [IA](#) de aprendizado profundo pré-treinado em uma grande quantidade de dados. Um LLM pode realizar várias tarefas, como responder a perguntas, resumir documentos, traduzir texto para outros idiomas e completar frases. Para obter mais informações, consulte [O que são LLMs](#).

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja [controle de acesso baseado em rótulo](#).

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja [7 Rs](#).

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também [endianness](#).

LLM

Veja [grande modelo de linguagem](#).

ambientes inferiores

Veja [ambiente](#).

M

machine learning (ML)

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

ramificação principal

Veja [ramificação](#).

Malware

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

Serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Veja [Programa de Aceleração da Migração](#).

mecanismo

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

conta de membro

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

MES

Veja [sistema de execução de manufatura](#).

Transporte de Telemetria de Enfileiramento de Mensagens (MQTT)

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

microsserviço

Um serviço pequeno e independente que se comunica de forma bem definida APIs e normalmente é de propriedade de equipes pequenas e independentes. Por exemplo, um sistema de seguradora pode incluir microsserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos microsserviços incluem agilidade, escalabilidade flexível, fácil implantação, código reutilizável e resiliência. Para obter mais informações, consulte [Integração de microsserviços usando serviços sem AWS servidor](#).

arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio

de uma interface bem definida usando leveza. APIs Cada microserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte [Implementação de microserviços em. AWS](#)

Programa de Aceleração da Migração (MAP)

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

migração em escala

O processo de mover a maior parte do portfólio de aplicações para a nuvem em ondas, com mais aplicações sendo movidas em um ritmo mais rápido a cada onda. Essa fase usa as práticas recomendadas e lições aprendidas nas fases anteriores para implementar uma fábrica de migração de equipes, ferramentas e processos para agilizar a migração de workloads por meio de automação e entrega ágeis. Esta é a terceira fase da [estratégia de migração para a AWS](#).

fábrica de migração

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

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

A abordagem usada para migrar uma workload para a Nuvem AWS. Para obter mais informações, veja a entrada [7 Rs](#) neste glossário e consulte [Mobilize sua organização para acelerar migrações em grande escala](#).

ML

Veja [machine learning](#).

modernização

Transformar uma aplicação desatualizada (herdada ou monolítica) e sua infraestrutura em um sistema ágil, elástico e altamente disponível na nuvem para reduzir custos, ganhar eficiência e aproveitar as inovações. Para obter mais informações, consulte [Strategy for modernizing applications in the Nuvem AWS](#).

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte [Evaluating modernization readiness for applications in the Nuvem AWS](#).

aplicações monolíticas (monólitos)

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

MPA

Veja [Avaliação do Portfólio para Migração](#).

MQTT

Veja [Transporte de Telemetria de Enfileiramento de Mensagens](#).

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja [controle de acesso de origem](#).

OAI

Veja [identidade de acesso de origem](#).

OCM

Veja [gerenciamento de alterações organizacionais](#).

migração offline

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

OI

Veja [integração de operações](#).

Ola

Veja [acordo de nível operacional](#).

migração online

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

OPC-UA

Veja [Open Process Communications - Unified Architecture](#).

Open Process Communications - Unified Architecture (OPC-UA)

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (TO)

Sistemas de hardware e software que trabalham com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas de

tecnologia da informação (TI) e tecnologia operacional (TO) é o foco principal das transformações da [Indústria 4.0](#).

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

Uma estrutura para gerenciar grandes transformações de negócios disruptivas de uma perspectiva de pessoas, cultura e liderança. O OCM ajuda as organizações a se prepararem e fazerem a transição para novos sistemas e estratégias, acelerando a adoção de alterações, abordando questões de transição e promovendo mudanças culturais e organizacionais. Na estratégia de AWS migração, essa estrutura é chamada de aceleração de pessoas, devido à velocidade de mudança exigida nos projetos de adoção da nuvem. Para obter mais informações, consulte o [guia do OCM](#).

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

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

ORR

Veja [análise de prontidão operacional](#).

OT

Veja [tecnologia operacional](#).

VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A [Arquitetura de Referência de AWS Segurança](#) recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja [informações de identificação pessoal](#).

manual

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

PLC

Veja [controlador lógico programável](#).

PLM

Veja [gerenciamento do ciclo de vida do produto](#).

política

Um objeto que pode definir permissões (veja [política baseada em identidade](#)), especificar condições de acesso (veja [política baseada em recurso](#)) ou definir as permissões máximas para todas as contas em uma organização no AWS Organizations (veja [política de controle de serviços](#)).

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pushdown de predicados

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

controle preventivo

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

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais

informações, consulte Entidade principal em [Termos e conceitos de perfis](#) na documentação do IAM.

Privacidade por design

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

zonas hospedadas privadas

Um contêiner que contém informações sobre como você deseja que o Amazon Route 53 responda às consultas de DNS para um domínio e seus subdomínios em um ou mais VPCs. Para obter mais informações, consulte [Como trabalhar com zonas hospedadas privadas](#) na documentação do Route 53.

controle proativo

Um [controle de segurança](#) desenvolvido para evitar a implantação de recursos não conformes. Esses controles verificam os recursos antes de serem provisionados. Se o recurso não estiver em conformidade com o controle, ele não será provisionado. Para obter mais informações, consulte o [guia de referência de controles](#) na AWS Control Tower documentação e consulte [Controles proativos](#) em Implementação de controles de segurança em AWS.

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja [ambiente](#).

controlador lógico programável (PLC)

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

encadeamento de prompts

Uso da saída de um prompt do [LLM](#) como entrada para o próximo prompt para gerar respostas melhores. Essa técnica é usada para dividir uma tarefa complexa em subtarefas, ou para refinar ou expandir iterativamente uma resposta preliminar. Isso ajuda a melhorar a precisão e a relevância das respostas de um modelo e permite resultados mais granulares e personalizados.

pseudonimização

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

publish/subscribe (pub/sub)

Um padrão que permite comunicações assíncronas entre microsserviços para melhorar a escalabilidade e a capacidade de resposta. Por exemplo, em um [MES](#) baseado em microsserviços, um microsserviço pode publicar mensagens de eventos em um canal em que outros microsserviços possam assinar. O sistema pode adicionar novos microsserviços sem alterar o serviço de publicação.

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

Veja [responsável, aprovador, consultado, informado \(RACI\)](#).

RAG

Veja [geração aumentada via recuperação](#).

ransomware

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

Matriz RASCI

Veja [responsável, aprovador, consultado, informado \(RACI\)](#).

RCAC

Veja [controle de acesso por linha e coluna](#).

réplica de leitura

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

Redefinir arquitetura

Veja [7 Rs](#).

objetivo de ponto de recuperação (RPO).

O máximo período de tempo aceitável desde o último ponto de recuperação de dados. Isso determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja [7 Rs](#).

Região

Uma coleção de AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter informações, consulte [Specify which Regiões da AWS your account can use](#).

regressão

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

redefinir a hospedagem

Veja [7 Rs](#).

versão

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

Veja [7 Rs](#).

redefinir a plataforma

Veja [7 Rs](#).

recomprar

Veja [7 Rs](#).

resiliência

A capacidade de uma aplicação de resistir ou se recuperar de interrupções. [Alta disponibilidade](#) e [recuperação de desastres](#) são considerações comuns ao planejar a resiliência na Nuvem AWS. Para obter mais informações, consulte [Nuvem AWS Resilience](#).

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja [7 Rs](#).

Retirada

Veja [7 Rs](#).

Geração Aumentada de Recuperação (RAG)

Uma tecnologia de [IA generativa](#) em que um [LLM](#) faz referência a uma fonte de dados autorizada que está fora de suas fontes de dados de treinamento antes de gerar uma resposta. Por exemplo, um modelo RAG pode realizar uma pesquisa semântica na base de conhecimento ou nos dados personalizados de uma organização. Para obter mais informações, consulte [O que é RAG \(geração aumentada via recuperação\)?](#).

alternância

O processo de atualizar periodicamente um [segredo](#) para dificultar o acesso de um invasor às credenciais.

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja [objetivo de ponto de recuperação](#).

RTO

Veja [objetivo de tempo de recuperação](#).

runbook

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

S

SAML 2.0

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

para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte [Sobre a federação baseada em SAML 2.0](#) na documentação do IAM.

SCADA

Veja [controle de supervisão e aquisição de dados](#).

SCP

Veja [política de controle de serviço](#).

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Consiste no valor secreto e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte [What's in a Secrets Manager secret?](#) na documentação do Secrets Manager.

segurança desde a concepção

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

controle de segurança

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

hardening da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização em AWS Organizations. SCPs defina barreiras ou estabeleça limites nas ações que um administrador pode delegar a usuários ou funções. Você pode usar SCPs como listas de permissão ou listas de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte [Políticas de controle de serviço](#) na AWS Organizations documentação.

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

Uma avaliação de um aspecto de performance de um serviço, como taxa de erro, disponibilidade ou throughput.

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme avaliado por um [indicador de nível de serviço](#).

modelo de responsabilidade compartilhada

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

SIEM

Veja [sistema de gerenciamento de eventos e informações de segurança](#).

ponto único de falha (SPOF)

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

SLA

Veja [acordo de serviço](#).

SLI

Veja [indicador de nível de serviço](#).

SLO

Veja [objetivo de nível de serviço](#).

split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte [Phased approach to modernizing applications in the Nuvem AWS](#).

SPOF

Veja [ponto único de falha](#).

esquema em estrela

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

padrão strangler fig

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

sub-rede

Um intervalo de endereços IP na VPC. Cada sub-rede fica alocada em uma única zona de disponibilidade.

controle supervisor e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

Testar um sistema de forma que simule as interações do usuário para detectar possíveis problemas ou monitorar a performance. Você pode usar o [Amazon CloudWatch Synthetics](#) para criar esses testes.

prompt do sistema

Uma técnica para fornecer contexto, instruções ou orientações a um [LLM](#) a fim de direcionar seu comportamento. Os prompts do sistema ajudam a definir o contexto e a estabelecer regras para interações com os usuários.

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja [ambiente](#).

treinamento

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

gateway de trânsito

Um hub de trânsito de rede que você pode usar para interconectar sua rede com VPCs a rede local. Para obter mais informações, consulte [O que é um gateway de trânsito](#) na AWS Transit Gateway documentação.

fluxo de trabalho baseado em troncos

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

Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas de

gerenciamento para você. Para obter mais informações, consulte [Usando AWS Organizations com outros AWS serviços](#) na AWS Organizations documentação.

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja [ambiente](#).

V

aspiração

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

controle de versões

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

emparelhamento da VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do

projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

WORM

Veja [gravação única e várias leituras](#).

WQF

Veja [AWS Workload Qualification Framework](#).

gravação única e várias leituras (WORM)

Um modelo de armazenamento que grava dados uma única vez e evita que os dados sejam excluídos ou modificados. Os usuários autorizados podem ler os dados quantas vezes forem necessárias, mas não podem alterá-los. Essa infraestrutura de armazenamento de dados é considerada [imutável](#).

Z

exploração de dia zero

Um ataque, normalmente malware, que tira proveito de uma [vulnerabilidade zero-day](#).

vulnerabilidade de dia zero

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

prompt zero shot

Fornecer a um [LLM](#) instruções para realizar uma tarefa, mas sem exemplos (shots) que possam ajudar a orientá-lo. O LLM deve usar seu conhecimento pré-treinado para lidar com a tarefa. A eficácia dos prompts zero-shot depende da complexidade da tarefa e da qualidade do prompt.

Veja também [prompts few-shot](#).

aplicação zumbi

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

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.