



Adotando o padrão Matter para fabricantes de dispositivos de IoT

AWS Orientação prescritiva



AWS Orientação prescritiva: Adotando o padrão Matter para fabricantes de dispositivos de IoT

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Introdução	1
Objetivos	1
Entendendo a questão	3
Protocolo de matéria	3
Visão geral de como o Matter funciona	4
Vantagens da certificação	5
Benefícios para os consumidores	5
Configuração simplificada e gerenciamento unificado	5
Escolha e flexibilidade aprimoradas no controle de voz	6
Benefícios para fabricantes de dispositivos	6
Certificação única em todos os ecossistemas	7
Custos de desenvolvimento reduzidos	7
Suporte ao cliente simplificado	7
Considerações sobre certificação	9
Protocolos de conectividade não IP	9
Limitações de hardware	10
Ecossistemas de clientes	10
Tipos de dispositivos ainda não definidos	11
Uma alternativa: proxy em gateways	11
Conectividade em nuvem com a Matter	13
Habilitando recursos avançados de dispositivos com conectividade em nuvem para terminais importantes	13
Casos de uso que exigem conectividade com a nuvem	13
Arquiteturas para permitir a conectividade na nuvem	14
Bridging Matter e plataformas de nuvem de fabricantes	15
Segurança	17
autenticação de dispositivos	17
Comunicação criptografada	17
O ver-the-air atualiza	17
Desenvolvimento com Matter	19
Usando a Alexa	19
CA privada da AWS suporte para Matter	19
Perguntas frequentes	21
Quais são os níveis de associação com o Matter?	21

Como os consumidores de casas inteligentes se beneficiam da Matter?	22
Como os fabricantes de dispositivos se beneficiam da Matter?	22
O Matter substitui o Wi-Fi, o Bluetooth ou o Thread?	22
O que é ID do fornecedor e ID do produto?	23
Quais dispositivos precisam ser certificados pela Matter?	23
Meu tipo de produto não está definido atualmente no Matter. Para quais tarefas adicionais devo reservar tempo para obter a certificação Matter dos produtos?	24
Alguns dos meus dispositivos se conectam diretamente à rede Wi-Fi doméstica. Esses dispositivos precisam ser certificados pela Matter?	24
Recursos	25
AWS recursos	25
Aliança de padrões de conectividade (CSA) para IoT	25
Histórico do documentos	26
Glossário	27
#	27
A	28
B	31
C	33
D	36
E	40
F	42
G	44
H	45
eu	47
L	49
M	50
O	55
P	57
Q	60
R	61
S	64
T	68
U	69
V	70
W	70
Z	71

Adotando o padrão Matter para fabricantes de dispositivos de IoT

Tushar Patel, Vijay Ujjain e David Walters, da Amazon Web Services (AWS)

Fevereiro de 2024 ([histórico do documento](#))

De acordo com o [Statista](#), espera-se que o número de residências inteligentes, em todo o mundo, chegue a 780 milhões até 2028. Esse rápido crescimento trouxe desafios em termos de operações e gerenciamento. Do ponto de vista do consumidor, cada fornecedor de dispositivos tem um método diferente de integrar o dispositivo doméstico inteligente em uma rede doméstica por meio de um aplicativo específico desse fornecedor de dispositivos. Isso dificulta o gerenciamento de uma variedade crescente de diversos tipos de dispositivos de vários fornecedores. Da mesma forma, do ponto de vista de um fabricante de dispositivos, certificar seus produtos domésticos inteligentes com vários ecossistemas aumenta o custo e a complexidade de seus processos de negócios. Por exemplo, isso pode exigir SKUs diferentes para o mesmo modelo de dispositivo. É uma sobrecarga adicional manter um aplicativo atraente de experiência do usuário e fornecer atualizações periódicas, retirando recursos do foco na criação e entrega de um produto melhor. Tanto os consumidores quanto os fabricantes de dispositivos se beneficiariam de um padrão comum de interoperabilidade para casas inteligentes. Esse padrão permite que dispositivos de vários fornecedores interoperem entre si de maneira perfeita, segura e confiável.

O novo padrão [Matter](#) apresenta uma excelente oportunidade para fabricantes de dispositivos de Internet das Coisas (IoT) no espaço de casas inteligentes. Esse padrão visa melhorar a compatibilidade e a interoperabilidade entre dispositivos de diferentes fabricantes. O Matter é um protocolo de conectividade residencial aberto e inteligente que permite a comunicação entre dispositivos de IoT, aplicativos móveis e serviços em nuvem.

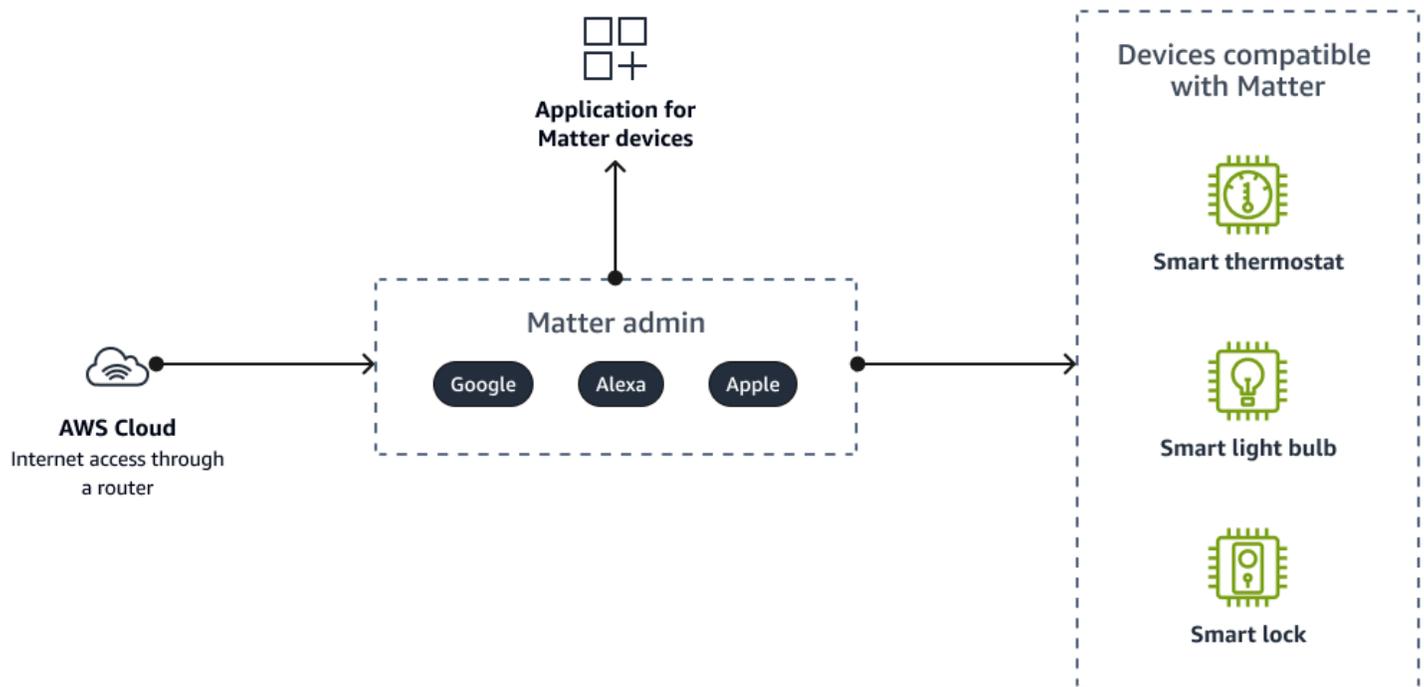
Objetivos

Ao integrar o padrão Matter em seus produtos, os fabricantes de dispositivos de IoT devem enfrentar vários desafios antes de iniciar o desenvolvimento. O Matter oferece muitas vantagens em relação aos protocolos de IoT proprietários, incluindo interoperabilidade, segurança, simplicidade, confiabilidade e dispositivos preparados para o futuro. No entanto, integrar o Matter em implantações de IoT novas e existentes requer planejamento e estratégia cuidadosos. Os fabricantes querem orientação sobre o processo de conformidade da Matter para aproveitar os benefícios e evitar

armadilhas. Este guia fornece aos fabricantes de dispositivos de IoT uma orientação abrangente sobre a adoção do Matter. Inclui um roteiro claro, da estratégia à implementação. Este guia facilita a transição para o Matter, ajudando você a criar produtos seguros, interoperáveis e prontos para o futuro que prosperam no ecossistema de casas inteligentes. Com a abordagem estratégica correta, as organizações podem superar os obstáculos da adoção da Matter e desenvolver dispositivos de IoT inovadores que adotem padrões abertos.

Este guia fornece aos fabricantes de dispositivos uma visão geral abrangente do Matter e as etapas necessárias para se tornarem compatíveis com o Matter. Ele descreve os prós e os contras do planejamento de uma estratégia de adoção do Matter. O guia também sugere as melhores práticas para aproveitar o Matter e, ao mesmo tempo, continuar a oferecer suporte aos protocolos sem fio existentes, de forma gradual. Para fabricantes de dispositivos de IoT que exploram soluções domésticas inteligentes, este guia pode informar sua estratégia de conectividade.

Entendendo o padrão Matter



Protocolo de matéria

O Matter é um protocolo de conectividade residencial aberto e inteligente que permite a comunicação entre dispositivos, aplicativos móveis e serviços em nuvem. Desenvolvido pela Connectivity Standards Alliance (CSA), o Matter simplifica a conectividade e a interoperabilidade para consumidores e fabricantes. O Matter oferece suporte a uma ampla variedade de categorias de casas inteligentes. Para os consumidores, a Matter fornece integração, gerenciamento unificado e controle em todos os ecossistemas. Para fabricantes, a Matter reduz os custos de desenvolvimento e suporte por meio de uma única certificação e do desenvolvimento de aplicativos. Muitas grandes empresas, como Amazon, Apple e Google, estão promovendo a adoção do Matter. A CSA oferece quatro [níveis de associação](#), dependendo do envolvimento da organização: promotores, participantes, adotantes e associados. Com forte apoio da indústria, a Matter visa fornecer conectividade perfeita entre marcas para consumidores e agilizar o desenvolvimento para fabricantes.

Visão geral de como o Matter funciona

O Matter é um protocolo baseado em IP em nível de aplicativo para dispositivos domésticos inteligentes em todos os ecossistemas de fornecedores. Ele funciona em dispositivos que usam IPv6. Conceitualmente, o Matter é organizado como uma coleção de nós de rede, que são endpoints do Matter. A seguir está um breve resumo da terminologia do Matter:

- Os dispositivos Matter são produtos domésticos inteligentes, como lâmpadas, interruptores, termostatos ou fechaduras.
- Uma malha Matter é a rede virtual na qual todos os dispositivos estão conectados. Todos os dispositivos compartilham a mesma raiz confiável. A estrutura forma uma topologia de rede em estrela.
- Um administrador do Matter cria, mantém e gerencia a segurança e os privilégios para todos os dispositivos na estrutura. Um administrador pode ser um hub ou um aplicativo. O Matter tem um recurso de vários administradores, em que um dispositivo Matter pode fazer parte de várias estruturas simultaneamente. Por exemplo, um único dispositivo Matter pode ser gerenciado tanto por um dispositivo Amazon Alexa quanto por um dispositivo Google Home, ambos podendo ser administradores do Matter na mesma rede física.
- Um comissário Matter é um dispositivo que comissiona (ou integra) um novo dispositivo Matter na estrutura. Pode ser um aplicativo em um telefone, um gateway doméstico inteligente ou um administrador do Matter.
- Uma ponte Matter conecta dispositivos de protocolo não IP a uma estrutura Matter.

Para obter informações sobre as diferentes funções que o hardware e o software podem assumir no Matter, consulte [Espreitando os bastidores da sua casa inteligente Matter](#) (postagem no blog da CSA).

Vantagens de se certificar com a Matter

A introdução do Matter promete oferecer vantagens significativas tanto para os consumidores de casas inteligentes quanto para os fabricantes que os atendem. Ao estabelecer uma linguagem comum para dispositivos inteligentes, a Matter visa desvendar o mercado fragmentado atual por meio de configuração simplificada, gerenciamento unificado entre plataformas e maior escolha e flexibilidade no controle de voz.

Para os consumidores, essa experiência unificada deve tornar a construção e a expansão de sua casa inteligente significativamente menos complexa e assustadora. Os fabricantes de dispositivos também obtêm benefícios significativos por meio de certificação simplificada, custos de desenvolvimento reduzidos e suporte simplificado ao cliente. Ambos os grupos se beneficiam, pois a Matter aumenta a interoperabilidade e reduz as barreiras à adoção de casas inteligentes. No geral, a certificação do padrão Matter está pronta para acelerar o crescimento do mercado de casas inteligentes, resolvendo problemas que o impediram até agora.

Tópicos

- [Benefícios da certificação Matter para consumidores domésticos inteligentes](#)
- [Benefícios da certificação Matter para fabricantes de dispositivos](#)

Benefícios da certificação Matter para consumidores domésticos inteligentes

A introdução do Matter promete oferecer benefícios significativos para os consumidores. O Matter fornece uma linguagem comum para que dispositivos domésticos inteligentes funcionem perfeitamente juntos nas principais plataformas. Ao certificar dispositivos com o Matter, os consumidores podem esperar uma configuração e gerenciamento mais simples de sua casa inteligente, bem como maior flexibilidade e escolha na forma como controlam seus dispositivos.

Configuração simplificada e gerenciamento unificado

Uma das maiores frustrações que os consumidores enfrentam são os complexos processos de configuração e integração necessários para operar diferentes dispositivos domésticos inteligentes e fazer com que trabalhem juntos. Cada dispositivo pode exigir seu próprio aplicativo proprietário e uma conta separada. Para resolver esse problema, o Matter habilita plug-and-play a funcionalidade

para dispositivos certificados. A integração de dispositivos certificados pela Matter é tão simples quanto conectar o dispositivo à rede doméstica local e usar o administrador do Matter, como o aplicativo Alexa, para ler o código QR no dispositivo.

Essa experiência de configuração unificada por meio de um único aplicativo significa que os consumidores não precisam mais manipular vários aplicativos separados para gerenciar diferentes marcas de dispositivos. Eles podem visualizar e controlar todas as luzes, travas, sensores e muito mais certificados pela Matter a partir de uma única interface. Todos os usuários da Apple HomeKit, Amazon Alexa e Google Assistant se beneficiam de poder descobrir e controlar dispositivos Matter sem precisar baixar aplicativos separados do fabricante. O gerenciamento simplificado de dispositivos domésticos inteligentes por meio de um sistema unificado reduz a complexidade para os consumidores e torna a criação e expansão de sua configuração muito menos assustadora.

Escolha e flexibilidade aprimoradas no controle de voz

O controle de voz se tornou uma forma popular de os consumidores interagirem com seus dispositivos domésticos inteligentes. No entanto, hoje em dia, a escolha do assistente de voz geralmente determina quais marcas de dispositivos você pode controlar com sua voz. A matéria muda isso ao permitir o controle de voz em todos os ecossistemas.

Os consumidores ganham a flexibilidade de escolher qual ecossistema de assistente de voz melhor atende às suas necessidades, sem precisar se preocupar com a compatibilidade do dispositivo. Um usuário confortável com o Google Assistant pode controlar seus dispositivos certificados pela Matter com sua voz, mesmo que os dispositivos tenham sido fabricados originalmente para a Alexa ou para mercados. HomeKit

Essa compatibilidade cruzada do controle de voz cria um ambiente mais aberto que oferece aos usuários mais opções. Eles podem escolher dispositivos com base em recursos e preços, em vez da compatibilidade com um único ecossistema. Se um usuário quiser mudar de assistente de voz no futuro, sua configuração de casa inteligente existente pode ser facilmente transferida com ele, pois todos os dispositivos falam o idioma comum da Matter.

Benefícios da certificação Matter para fabricantes de dispositivos

Além de ajudar os consumidores, a certificação Matter também oferece benefícios significativos aos fabricantes de dispositivos inteligentes. Ao adotar o padrão Matter, as organizações podem obter vantagens que reduzem custos e expandem o alcance de seus clientes.

Certificação única em todos os ecossistemas

Atualmente, para garantir a compatibilidade entre ecossistemas como Alexa HomeKit e Google Home, os fabricantes precisam passar por vários processos de certificação longos e caros com cada organização. A Matter muda isso estabelecendo uma única certificação comum.

Os fabricantes de dispositivos só precisam certificar seus produtos uma vez de acordo com o padrão Matter para serem compatíveis com todos os principais ecossistemas domésticos inteligentes e assistentes de voz. Isso simplifica o desenvolvimento e reduz significativamente os custos de certificação em comparação com o status quo. Os recursos não precisam mais ser gastos na manutenção de certificações separadas à medida que os produtos são atualizados. Uma única certificação Matter também prepara os produtos para o futuro e garante a compatibilidade mesmo com o surgimento de novos ecossistemas.

Custos de desenvolvimento reduzidos

A matéria também ajuda a reduzir os custos de desenvolvimento para os fabricantes. Ao adotar um padrão comum de conectividade e segurança, as organizações se beneficiam de componentes de infraestrutura compartilhada que contribuem para o projeto geral da Matter.

Por exemplo, os fabricantes não precisam mais incluir seus próprios roteadores Thread border nos produtos, transferindo essa responsabilidade para os fabricantes de hubs. Drivers e bibliotecas compartilhados e de código aberto reduzem ainda mais o trabalho redundante de engenharia. Mecanismos comuns de descoberta de serviços e configuração de dispositivos significam que é necessário menos desenvolvimento de aplicativos personalizados. Essas reduções nos custos de infraestrutura e desenvolvimento de aplicativos podem ser repassadas aos consumidores na forma de dispositivos domésticos inteligentes mais acessíveis.

Suporte ao cliente simplificado

A atual fragmentação no mercado de casas inteligentes gera altos encargos de suporte ao cliente para os fabricantes. Os consumidores frequentemente encontram problemas de conectividade, configuração e compatibilidade que exigem solução de problemas. A Matter visa reduzir esses problemas padronizando as funções principais.

Quando ocorrem problemas, os protocolos comuns subjacentes da Matter significam que as empresas podem diagnosticar e resolver problemas de conectividade com mais facilidade sem precisar considerar vários ecossistemas. Isso simplifica o processo de suporte. Com um único aplicativo e compatibilidade de voz comum, os clientes também têm mais facilidade em aprender a

usar dispositivos, reduzindo a necessidade de suporte em muitos casos. A experiência simplificada do cliente e a solução de problemas possibilitadas pela Matter ajudam a reduzir os custos de suporte de longo prazo para os fabricantes.

Considerações sobre a estratégia de certificação da Matter

O Matter permite a interoperabilidade entre diferentes dispositivos e plataformas domésticas inteligentes. No entanto, a certificação com a Matter nem sempre é a melhor escolha para fabricantes de dispositivos. Os custos de implementação e certificação podem não fazer sentido prático ou financeiro, dependendo do tipo de dispositivo e dos casos de uso. Esta seção explora alguns dos principais motivos pelos quais um fabricante pode optar por não certificar determinados dispositivos com o Matter.

Embora o padrão Matter tenha como objetivo simplificar o desenvolvimento e permitir a compatibilidade universal, certos tipos de dispositivos domésticos inteligentes podem enfrentar barreiras práticas à certificação que superam os benefícios. Para produtos com restrições rigorosas, protocolos não IP, públicos limitados ou tipos de dispositivos não definidos no Matter, buscar a certificação Matter pode não ser a melhor estratégia inicialmente. Esses podem ser os motivos pelos quais um fabricante pode evitar a adoção do Matter. No entanto, o Matter permite que dispositivos de gateway habilitados para IP façam proxy para endpoints não IP. Para certos dispositivos legados, uma abordagem de gateway pode ser um caminho viável para a compatibilidade com o Matter, evitando uma reformulação completa do dispositivo.

À medida que o padrão Matter evolui e seu escopo se expande para cobrir mais casos de uso, a necessidade de certificação pode se fortalecer com o tempo, mesmo para essas categorias de produtos. Os fabricantes de dispositivos precisam avaliar suas situações e roteiros específicos para determinar a melhor abordagem em relação à conformidade com a Matter. Em muitas situações, pode haver motivos técnicos ou comerciais sólidos para optar por não receber a certificação, pelo menos temporariamente.

Protocolos de conectividade não IP

Para adotar o padrão Matter, os dispositivos devem operar em redes IP, como Wi-Fi, Ethernet e Thread. Protocolos sem fio não IP, como Zigbee, Z-Wave e Bluetooth LE, são comumente usados em dispositivos de baixa largura de banda. Esses protocolos exigem um tradutor de protocolo adicional não baseado em IP para IP para serem compatíveis com o Matter. A atualização do módulo de comunicação ou a introdução de um gateway de tradução normalmente aumenta o custo de hardware do dispositivo.

Adicionar suporte à pilha IP significa alocar mais memória e poder de processamento para o manuseio da rede. Isso pode exceder as capacidades de dispositivos de custo extremamente

baixo e baixo consumo de energia. A adição de memória extra ou flash para suportar IP também aumentaria os custos de fabricação e reduziria a vida útil da bateria. Para casos de uso em que ligar e desligar dados de energia ou sensores são tudo o que é necessário, os protocolos não IP podem fornecer uma solução eficiente.

A Matter basicamente exclui a certificação de qualquer dispositivo que dependa de padrões sem fio proprietários e não IP. Isso pode limitar os fabricantes que desejam usar métodos alternativos de conectividade para seus produtos de baixo custo. Embora protocolos baseados em IP, como Wi-Fi e Ethernet, sejam necessários para a interface de diferentes ecossistemas, os padrões não IP ainda têm mérito para a conectividade básica de sensores e comutadores em algumas aplicações.

Limitações de hardware

Outro desafio é que o Matter exige um nível mínimo de capacidade de processamento e memória no dispositivo para suportar a pilha de software necessária. No entanto, os dispositivos domésticos inteligentes mais básicos geralmente têm recursos de chip incorporados muito limitados, devido a restrições de custo e tamanho.

Por exemplo, um sensor simples de porta ou janela pode conter somente um microcontrolador com menos de 100 KB de memória flash e 10 KB de RAM. Isso não fornece espaço suficiente de armazenamento e processamento para uma implementação completa do Matter. Adicionar silício mais poderoso e caro aumentaria significativamente as listas de materiais.

Nos casos em que custo e tamanho são as principais prioridades, os fabricantes podem achar que os requisitos da Matter não estão alinhados com seus orçamentos de hardware. A certificação de sensores, comutadores ou controladores muito básicos com o Matter pode forçar atualizações de hardware desnecessárias que afetam a acessibilidade.

Ecossistemas de clientes

Outro fator a ser considerado é se a base de clientes-alvo de um fabricante usa plataformas domésticas inteligentes compatíveis com o Matter. Se a maioria dos consumidores desse segmento não usar controladores Matter ou hubs e aplicativos compatíveis com Matter, pode haver pouco incentivo para certificar produtos.

Por exemplo, uma empresa focada em atender às necessidades de usuários idosos pode descobrir que seus clientes têm configurações simples sem os administradores do Matter. Ou os entusiastas

da automação residencial do-it-yourself (DIY) podem preferir soluções personalizadas e não precisam da plug-and-play experiência da Matter em todas as marcas.

Em cenários em que o público-alvo não interage com a infraestrutura da Matter, a certificação aumenta a complexidade sem benefícios claros. Os recursos podem ser mais bem gastos na otimização da experiência do usuário nas plataformas relevantes, em vez de desviar os esforços para a conformidade com a Matter.

Tipos de dispositivos ainda não definidos

Atualmente, a Matter define apenas perfis e especificações de dispositivos para categorias comuns de casas inteligentes, como iluminação, HVAC, fechaduras, persianas e entretenimento. Qualquer tipo de produto de nicho fora dessas áreas definidas precisa usar um perfil personalizado até que o tipo de dispositivo seja padronizado. Categorias de dispositivos fora das verticais listadas, como controladores de irrigação, equipamentos de piscina e aparelhos de nicho, ainda não podem usar o Matter.

Se uma empresa desenvolve tipos de dispositivos exclusivos que não são cobertos pelos perfis existentes do Matter, a certificação não é possível até que novos perfis sejam elaborados. Isso pode atrasar o lançamento de um novo produto enquanto espera que a Matter expanda seu escopo.

Em vez de adiar o lançamento de inovações, alguns fabricantes podem preferir levar soluções de nicho ao mercado mais cedo por meios proprietários. A certificação posterior ainda é uma opção após o vencimento dos perfis relevantes. Para vantagens de ser pioneiro, usar o direct-to-consumer Matter pode ser preferível em alguns casos.

Uma alternativa: proxy em gateways

Em situações em que um dispositivo de endpoint tem limitações que impedem a certificação direta da Matter, uma abordagem alternativa é colocar a capacidade Matter do dispositivo em um gateway. O gateway serve como uma ponte que faz a tradução entre o protocolo sem fio local do endpoint e o protocolo Matter baseado em IP.

Por exemplo, um sensor de temperatura básico se comunicando por meio de um padrão de rádio proprietário ainda pode aparecer como um dispositivo Matter para o administrador do Matter. O gateway recebe dados do sensor em uma interface não IP, mas expõe entidades virtuais da Matter que representam esses dados por IP aos controladores. Isso permite que você use o hardware existente e obtenha alguns benefícios de interoperabilidade por meio do gateway.

Obviamente, isso aumenta a complexidade para os desenvolvedores e requer gateways para suportar a camada de tradução necessária. Mas pode ser um compromisso viável nos casos em que a certificação direta é muito desafiadora para o próprio dispositivo. Os proxies podem ajudar soluções de baixo consumo de energia ou de nicho a participarem dos ecossistemas da Matter sem uma revisão completa do hardware.

Conectividade em nuvem com a Matter

Embora o Matter permita a interoperabilidade básica de dispositivos locais, é necessária conectividade adicional na nuvem para fornecer over-the-air atualizações robustas, dados de telemetria, gerenciamento remoto e integração com serviços proprietários de fornecedores. Os fabricantes de dispositivos têm opções, como enviar um hub de gateway Matter, usar um hub doméstico certificado pela Matter ou integrar a conectividade direta à nuvem aos endpoints. Os padrões para atter-to-cloud conectividade M estão surgindo, mas os fabricantes ainda precisam integrar pilhas adicionais de software de conectividade aos dispositivos Matter. Oferecer o valor total dos dispositivos domésticos inteligentes em áreas como diagnósticos e atualizações de novos recursos exige que os fabricantes da Matter considerem a integração na nuvem, além da operação local básica.

Habilitando recursos avançados de dispositivos com conectividade em nuvem para terminais importantes

O padrão Matter promete unificar dispositivos de IoT de diferentes fornecedores por meio de um protocolo comum. Ele especifica como os dispositivos domésticos inteligentes descobrem, se comunicam e interoperam entre si na rede local usando tecnologias de rede baseadas em IP, como Ethernet, Wi-Fi e Thread. Essa interoperabilidade local permite que dispositivos certificados pela Matter de diferentes fornecedores trabalhem juntos perfeitamente em atividades como cenas automatizadas e controle de voz. No entanto, o Matter não define interfaces de nuvem nem exige conectividade com a Internet para os terminais do dispositivo.

Atualmente, muitos dispositivos inteligentes dependem de conectividade adicional na nuvem para os principais recursos, como atualizações over-the-air (OTA), acesso remoto e integrações com plataformas de fabricantes. Os fabricantes de dispositivos que desejam criar produtos compatíveis com o Matter, mantendo a funcionalidade avançada, enfrentam algumas considerações de design para complementar o Matter com conectividade em nuvem. Embora o controle local básico e a integração do assistente de voz funcionem para dispositivos Matter simples, é necessária conectividade adicional na nuvem para permitir recursos mais avançados.

Casos de uso que exigem conectividade com a nuvem

Embora o Matter gerencie a interoperabilidade de dispositivos locais, a conectividade adicional na nuvem permite vários recursos importantes de dispositivos domésticos inteligentes:

- **Atualizações O ver-the-air (OTA)** — A entrega de atualizações de firmware e software pela Internet permite que os fornecedores aprimorem facilmente os dispositivos que já estão implantados. Sem o OTA, as atualizações seriam feitas manualmente. Embora o padrão Matter descreva como as atualizações OTA são tratadas e entregues aos endpoints certificados pela Matter, ele depende da funcionalidade suportada pelo hub Matter ao qual o endpoint está conectado. Além disso, há restrições sobre quais atualizações são fornecidas ao endpoint. Por exemplo, quando o endpoint solicita uma atualização, somente a atualização mais recente disponível é fornecida. Todos os dispositivos do mesmo tipo recebem essa única atualização. Não há opção de fazer uma atualização sequencial ou mesmo uma reversão OTA ou exclusão de uma atualização. Habilitar a conectividade em nuvem no endpoint pode mitigar essa falta de gerenciamento refinado das atualizações do OTA.
- **Acesso e controle remotos** — acessar e controlar dispositivos remotamente de fora da rede doméstica requer um endpoint na nuvem. O Matter, conforme definido atualmente, suporta apenas acesso local. Embora um endpoint Matter possa ser controlado com um aplicativo de usuário dentro da rede local, o controle remoto só está disponível se for suportado pelo hub Matter. Mesmo assim, normalmente, apenas controles remotos básicos estão disponíveis.
- **Telemetria e diagnóstico** — A agregação de dados de campo, como registros de erros e fluxos de sensores, na nuvem permite que os fornecedores monitorem a integridade dos dispositivos e identifiquem problemas. Embora o Matter ofereça suporte a diagnósticos relacionados a rádio e protocolos por meio do cluster de diagnóstico geral, qualquer diagnóstico detalhado específico do dispositivo requer conectividade com a nuvem para que o fabricante possa recuperar dados do dispositivo.
- **Integrações específicas do fornecedor** — Todos os recursos e tipos de dados personalizados que não estão definidos na especificação Matter exigem conectividade com as plataformas de nuvem do fornecedor.
- **Integrações externas** — A vinculação a serviços de terceiros, como assistentes de voz que não estão no ecossistema Matter ou gateways de pagamento de terceiros (conforme necessário por caso de uso), requer conectividade com a Internet além do administrador do Matter.

Com esses recursos essenciais que dependem da conectividade em nuvem, os endpoints da Matter geralmente precisam de opções adicionais para acesso à Internet.

Arquiteturas para permitir a conectividade na nuvem

Para dispositivos Matter, existem três abordagens gerais para fornecer a conectividade de nuvem necessária e, ao mesmo tempo, atender às especificações de operação local.

Hub doméstico inteligente com gateway integrado

Alguns fabricantes de dispositivos podem optar por enviar um hub doméstico proprietário que incorpore o administrador do Matter e um gateway para seus serviços em nuvem. Esse hub doméstico gerenciaria os endpoints Matter conectados localmente de acordo com o padrão, além de facilitar as conexões em nuvem para funções avançadas. O hub pode suportar atualizações OTA, acesso remoto e coleta de telemetria para endpoints.

Transfira a conectividade da nuvem para um hub Matter existente

Em vez de agrupar um hub personalizado, os dispositivos podem ser projetados para se conectar a hubs Matter, como Amazon Echo ou Google Home, para conectividade com a Internet. Nesse caso, o hub Matter existente lida com a comunicação do dispositivo local de acordo com o padrão e também fornece um gateway para a nuvem para os endpoints que precisam dela. Isso aproveita a infraestrutura que os consumidores talvez já tenham. No entanto, essa abordagem depende do nível de suporte oferecido pelo hub Matter para recursos que não são especificados como normativos para hubs Matter no padrão.

Conectividade direta à nuvem em endpoints

Dispositivos com conectividade direta à Internet, como Wi-Fi, podem integrar conectividade separada para a rede local Matter e para os serviços em nuvem do fornecedor. Isso permite que o dispositivo atue como seu próprio gateway para a nuvem. No entanto, são necessárias soluções para endpoints não Wi-Fi que dependem de protocolos como o Thread. Isso permite que os dispositivos se conectem à nuvem de forma independente, mas pode não ser viável para dispositivos simples, de baixo custo e alimentados por bateria.

Bridging Matter e plataformas de nuvem de fabricantes

Embora o Matter simplifique a interoperabilidade local, é necessário um esforço adicional para conectar facilmente os sistemas de administração do Matter e as plataformas de nuvem do fabricante. Organizações como a Connectivity Standards Alliance (CSA) estão trabalhando para padronizar a forma como os dispositivos Matter interagem com a nuvem para recursos como atualizações OTA. A adoção ampla de padrões para essa conectividade em nuvem facilitaria o desenvolvimento para fabricantes de dispositivos.

O caminho ideal depende dos casos de uso, dos preços e dos modelos de negócios de produtos específicos. É claro que o acesso robusto aos serviços em nuvem é necessário para liberar toda a funcionalidade que os consumidores de casas inteligentes esperam, mesmo para dispositivos

compatíveis com Matter que se concentram na interoperabilidade local. Os fabricantes de dispositivos têm a oportunidade de usar o Matter para interoperabilidade e, ao mesmo tempo, fornecer recursos avançados por meio de conectividade em nuvem cuidadosamente projetada.

Segurança

Segurança por design é a prática de incorporar funções de segurança durante o estágio de design do dispositivo, e não como uma reflexão tardia durante os estágios posteriores do desenvolvimento. A comunicação criptografada e as atualizações over-the-air (OTA) são exemplos de segurança por design. A Matter fornece uma base sólida para dispositivos domésticos inteligentes implementando a segurança desde o design, começando em uma instalação de fabricação confiável e segura. Os dispositivos Matter só podem ser fabricados e provisionados por proprietários de uma autoridade certificadora (CA) conhecida e confiável da Autoridade de Atestado de Produto (PAA).

autenticação de dispositivos

Os dispositivos Matter devem se autenticar entre si e com um controlador antes de poderem se comunicar. Somente dispositivos autorizados podem se conectar à malha Matter. Durante a fabricação, os dispositivos são provisionados com uma identidade exclusiva e um certificado X.509, conhecido como Certificado de Atestado de Dispositivo (DAC). Quando o dispositivo tenta se conectar à estrutura Matter pela primeira vez, o dispositivo do comissário verifica a validade do DAC e se ele está assinado por uma CA conhecida e confiável do Product Attestation Intermediate (PAI). O dispositivo do comissário também verifica se o dispositivo que está tentando se conectar à rede segue as especificações, protocolos e padrões de segurança da Matter. O dispositivo tem acesso à estrutura Matter somente se todas as verificações forem bem-sucedidas.

Comunicação criptografada

Depois que o dispositivo recebe acesso à estrutura Matter, todos os dados transmitidos entre os dispositivos são protegidos por uma criptografia forte. A integridade dos dados é preservada usando uma abordagem de vários níveis. O comissário do Matter realiza a troca de chaves e a verificação de assinaturas usando a curva ECC-256 secp256r1. Depois que as chaves são trocadas, os dispositivos Matter criptografam os dados em trânsito usando o AES-256. Para cada mensagem, os dispositivos usam o algoritmo SHA-256 para verificar se os dados não foram adulterados durante a transmissão.

O ver-the-air atualiza

O padrão Matter também exige que os dispositivos implementem uma postura de segurança robusta para atualizações over-the-air (OTA). O OTA é uma parte essencial de um ecossistema

doméstico inteligente para que os dispositivos possam receber atualizações de segurança junto com novos recursos. Cada atualização de firmware para dispositivos Matter deve ser assinada pela chave privada do fabricante. O dispositivo verifica a assinatura da carga usando a chave pública assimétrica correspondente. Depois que a assinatura da carga for verificada, o dispositivo poderá confirmar a imagem em seu carregador de inicialização e reiniciá-la. Durante o processo de inicialização, o dispositivo deve verificar novamente a imagem para garantir que ela não tenha sido adulterada, e o dispositivo também verifica se está executando a versão mais recente conhecida.

Desenvolvimento com Matter

Usando a Alexa

A Amazon oferece um conjunto abrangente de ferramentas para o desenvolvimento do Matter. Essas ferramentas fornecem um caminho rápido para criar produtos Matter que sejam compatíveis com todos os principais ecossistemas e que funcionem perfeitamente com o Amazon Alexa.

Programa: Funciona com Alexa

Esse programa garante que seus dispositivos conectados à Alexa ofereçam uma ótima experiência ao cliente. O selo Works with Alexa (WWA) aumenta a confiança do cliente, o que ajuda a impulsionar a preferência por seus dispositivos certificados. Para obter mais informações, consulte [Anunciando o lançamento do Matter e apresentando trabalhos com a Alexa \(WWA\) para dispositivos Matter](#) (postagem no blog da Amazon).

SDK: Desenvolva o Matter com a Alexa

Esse SDK permite que você adicione conectividade Matter local ao seu dispositivo, além de incluir conectividade gerenciada em nuvem, business intelligence e suporte OTA. Para obter mais informações, consulte [Tire o máximo proveito do Matter com a Alexa](#).

Kit: Kit para desenvolvedores Alexa Ambient Home

Esse kit ajuda você a se integrar a dispositivos de vários protocolos para criar um ambiente e uma casa inteligente unificada com a Alexa. Para obter mais informações, consulte [Amazon Alexa](#).

Ponto final: Ponto final comissionável

Para dispositivos Matter conectados por habilidades, a API Commissionable Endpoint cria uma conexão local baseada em Matter com dispositivos Alexa sem nenhuma etapa exigida pelo cliente com a permissão dele. Para obter mais informações, consulte [Alexa.Commissionable Interface 1.0](#) (Alexa Skills Kit).

CA privada da AWS suporte para Matter

AWS Private Certificate Authority (CA privada da AWS) fornece orientação sobre o uso do padrão Matter.

DAC para Matter

O Matter exige um certificado de atestado de dispositivo (DAC), que deve ser emitido por uma CA de atestado de dispositivo compatível com a política de certificado (CP) da infraestrutura de chave pública (PKI) da Matter. Os fornecedores de dispositivos podem usar CA privada da AWS para fazer o seguinte:

- Hospede a autoridade de certificação (CA) da Autoridade de Atestado de Produto (PAA)
- Hospede a CA do Product Attestation Intermediate (PAI)
- Emita, assine e mantenha o DAC de cada dispositivo

Para obter mais informações, consulte [Usar AWS Private Certificate Authority para emitir certificados de atestado de dispositivo para o Matter](#) no Blog AWS de Segurança.

Infraestrutura para Matter

AWS fornece um exemplo que demonstra o uso de [AWS Cloud Development Kit \(AWS CDK\)](#) para configurar a infraestrutura de PKI para o Matter. Você usa CA privada da AWS para atender aos requisitos do Matter PKI CP. Para obter mais informações, consulte o [projeto Matter PKI CDK](#) em GitHub

Amostras de Java

CA privada da AWS fornece exemplos de Java para criar certificados de Autoridade de Atestado de Produto (PAA), certificados de Atestado de Produto Intermediário (PAI) e Certificados de Atestado de Dispositivo (DACs) compatíveis com o Matter. Para obter mais informações, consulte [Usando a CA privada da AWS API para implementar o padrão Matter \(exemplos de Java\)](#) na AWS Private Certificate Authority documentação.

Guia para conformidade com Matter PKI

Este [Guia de Conformidade do Matter PKI](#) explica como implementar e demonstrar a conformidade com os requisitos do CSA Matter PKI CP. Ele fornece informações sobre como você pode usar para CA privada da AWS criar e operar Autoridades de Certificação (CAs) compatíveis com o Matter.

Perguntas frequentes

Quais são os níveis de associação com o Matter?

Em janeiro de 2023, a Matter tinha os seguintes quatro níveis de associação.

Tipo de membro	Taxa anual de associação (USD)	Descrição
Promotor	\$105.000	Lidere a aliança com aprovação final em todos os padrões, tenha um assento no conselho e participe dos comitês do conselho
Participante	\$20.000	Contribua com os padrões e acesse projetos de especificações para entrar no mercado mais rapidamente
Adotante	\$7.000	Use especificações aprovadas para criar e certificar produtos
Associado	\$0*	Rotule um produto certificado por meio do programa de transferência de certificação

*Para membros associados que rotulam em branco ou alteram a marca de um produto, isso custa uma taxa inicial de \$2.500 (USD) por produto e uma taxa contínua de \$500 por produto por ano.

O nível de associação escolhido depende do seu interesse em certificar um produto (adotante) ou definir o tipo de produto dentro do padrão (participante). Para obter mais informações sobre os níveis de associação, consulte [Impactar o futuro da IoT no site](#) da CSA.

Como os consumidores de casas inteligentes se beneficiam da Matter?

Os consumidores se beneficiam da Matter das seguintes formas:

- Integração simplificada de um dispositivo Matter em casa
- Gerenciamento unificado de todos os dispositivos domésticos inteligentes por meio de um único aplicativo
- Controle de dispositivos a partir de um ou mais assistentes de voz de diferentes ecossistemas

Para obter mais informações, consulte [Benefícios da certificação Matter para consumidores domésticos inteligentes](#) neste guia.

Como os fabricantes de dispositivos se beneficiam da Matter?

Os fabricantes de dispositivos se beneficiam da Matter das seguintes maneiras:

- Uma única certificação para um dispositivo em vez de várias certificações com cada ecossistema, como Amazon Alexa ou Google Home.
- O desenvolvimento do aplicativo não é mais necessário
- Custos reduzidos de materiais devido à não necessidade de enviar os elementos da infraestrutura (como um Thread Border Router)
- Custos reduzidos de suporte a clientes com problemas de infraestrutura e conectividade

Para obter mais informações, consulte [Benefícios da certificação Matter para fabricantes de dispositivos](#) neste guia.

O Matter substitui o Wi-Fi, o Bluetooth ou o Thread?

Não, o Matter é um protocolo em nível de aplicativo executado em redes IP. Dispositivos que usam Wi-Fi, Ethernet ou Thread para conectividade podem se tornar certificados pela Matter. A tabela a seguir resume como o Matter se compara com Wi-Fi, Bluetooth e Thread.

Atributo	Matéria	Wi-Fi	Bluetooth	Thread
Finalidade	Comunicação doméstica inteligente	Acesso à Internet e transferência de dados	Comunicação sem fio de curto alcance	Rede de malha sem fio de baixa potência
Intervalo	Varia de acordo com o protocolo subjacente	Até 300 pés	Até 30 pés	Até 300 pés
Largura de banda	Varia de acordo com o protocolo subjacente	Até 10 gigabits por segundo	Até 2 megabits por segundo	Até 250 kilobits por segundo
Consumo de energia	Varia de acordo com o protocolo subjacente	Relativamente alto	Relativamente baixo	Muito baixo
Segurança	Varia de acordo com o protocolo subjacente	WPA2, WPA3	Conexões seguras AES, BLE	AES
Custo	Varia de acordo com o dispositivo	Relativamente barato	Relativamente barato	Relativamente caro

O que é ID do fornecedor e ID do produto?

Os membros da CSA podem solicitar um ID de fornecedor que os identifique como fornecedor. Os produtos da empresa são doravante atribuídos a esse ID e podem ser rastreados até sua origem. Além disso, eles recebem um ID de produto exclusivo. O código numérico de 16 dígitos acompanha produtos como o número do passaporte e os torna tão inconfundíveis quanto o fornecedor.

Quais dispositivos precisam ser certificados pela Matter?

Qualquer dispositivo que precise ser autenticado e fazer parte da estrutura Matter precisa ser certificado pela Matter. No entanto, os dispositivos projetados para interagir somente com o

hub especificado pelo fornecedor por meio de um protocolo não padrão (proprietário) não se beneficiariam do processo de certificação da Matter. Por exemplo, um hub de sistema de segurança residencial inteligente deve ser certificado como compatível com a Matter, mas um sensor de porta ou janela que se comunica com o hub não precisa ser certificado como compatível com a Matter. A escolha de obter um produto certificado para a Matter é motivada principalmente por essa consideração.

Meu tipo de produto não está definido atualmente no Matter. Para quais tarefas adicionais devo reservar tempo para obter a certificação Matter dos produtos?

As especificações do Matter não são compatíveis com todos os tipos de dispositivos. Se o seu tipo de dispositivo não for compatível, a primeira etapa é ingressar no CSA como participante. Isso requer seu investimento financeiro e de tempo no CSA. Como membro participante, você lidera a definição dos tipos de dispositivos e tem acesso aos rascunhos de especificações que permitem uma go-to-market estratégia mais rápida. Para obter mais informações sobre os níveis de associação, consulte [Impactar o futuro da IoT no site](#) da CSA.

Alguns dos meus dispositivos se conectam diretamente à rede Wi-Fi doméstica. Esses dispositivos precisam ser certificados pela Matter?

A certificação Matter pode beneficiar dispositivos que se conectam diretamente à rede doméstica inteligente porque podem se conectar à malha Matter. Isso permite que os consumidores controlem os dispositivos por meio de seus assistentes virtuais na mesma estrutura Matter. No entanto, os consumidores devem usar um aplicativo específico do dispositivo para qualquer operação que seja específica do fornecedor e não esteja definida na especificação Matter.

Recursos

AWS recursos

- [Aproveite ao máximo o Matter com a Alexa](#)
- [Anunciando o lançamento do Matter e apresentando o Works with Alexa \(WWA\) para dispositivos Matter \(blog da Amazon Alexa\)](#)

Aliança de padrões de conectividade (CSA) para IoT

- [Site da CSA](#)
- [Visão geral do processo de certificação CSA](#)
- [Provedores de testes autorizados pela CSA](#)
- [Especificações do assunto](#)

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	—	5 de fevereiro de 2024

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: migre seu banco de dados Oracle local para a edição compatível com o Amazon Aurora 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: Migre seu banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) for Oracle no. Nuvem AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migre seu sistema de gerenciamento de relacionamento com o cliente (CRM) para a 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: Migre seu banco de dados Oracle local para o Oracle em uma EC2 instância no. 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 local para um serviço em 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 atributos](#).

serviços abstratos

Veja os [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 no qual 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.

função agregada

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 a [inteligência artificial](#).

AIOps

Veja as [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 aplicativos

Uma abordagem de segurança que permite o uso somente de aplicativos aprovados 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 ruim

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

BCP

Veja o [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 do aplicativo em um ambiente (azul) e a nova versão do aplicativo no outro ambiente (verde). Essa estratégia ajuda você a reverter rapidamente com o mínimo de impacto.

bot

Um aplicativo de software que executa tarefas automatizadas pela Internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como rastreadores da Web que indexam informações na Internet. Alguns outros bots, conhecidos como bots ruins, têm como objetivo perturbar ou causar danos a indivíduos ou organizações.

botnet

Redes de [bots](#) infectadas por [malware](#) e sob o controle de uma única parte, conhecidas como pastor de bots ou operador de bots. As redes de bots 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 em vidro quebrado

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 [Implementar procedimentos de quebra de vidro na orientação do Well-Architected](#) AWS .

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

Consulte [Estrutura de adoção da AWS nuvem](#).

implantação canária

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substituirá a versão atual em sua totalidade.

CCoE

Veja o [Centro de Excelência em Nuvem](#).

CDC

Veja [a captura de dados de alterações](#).

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 a [integração e a 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 CCo E](#) no Blog de Estratégia Nuvem AWS Empresarial.

computação em nuvem

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

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 quando migram para o 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

Consulte o [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 GitHub ou 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 da [IA](#) que usa aprendizado de máquina para analisar e extrair informações de formatos visuais, como imagens e vídeos digitais. Por exemplo, a Amazon SageMaker AI fornece algoritmos de processamento de imagem para CV.

desvio de configuração

Para uma carga de trabalho, uma alteração de configuração em relação ao estado esperado. Isso pode fazer com que a carga de trabalho 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

Um conjunto 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 is commonly described as a 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.

malha de dados

Uma estrutura arquitetônica 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 que oferece suporte à inteligência comercial, como análises. 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

Consulte a [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 o [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 são comumente 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 a [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 a [recuperação de desastres](#).

detecção de deriva

Rastreando desvios de uma configuração básica. 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 o [mapeamento do fluxo de valor do desenvolvimento](#).

E

EDA

Veja a [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 à [computação em nuvem](#), a computação de ponta 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 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 o [endpoint do 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 corporativos (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 pipeline de CI/CD, 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 o [planejamento de recursos corporativos](#).

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](#). Ele armazena dados quantitativos sobre as operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: aquelas que contêm medidas e aquelas que contêm uma chave externa para uma tabela de dimensões.

falham rapidamente

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

limite de isolamento de 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 [Limites de isolamento de AWS falhas](#).

ramificação de recursos

Veja a [filial](#).

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.

solicitação rápida

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 contextual, em que os modelos aprendem com exemplos (fotos) incorporados aos prompts. Solicitações rápidas podem ser eficazes para tarefas que exigem formatação, raciocínio ou conhecimento de domínio específicos. Veja também a solicitação [zero-shot](#).

FGAC

Veja o [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 por meio da [captura de dados alterados](#) para migrar 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 o [modelo da fundação](#).

modelo de fundação (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 básicos](#).

G

IA generativa

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

bloqueio geográfico

Veja as [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 baseado em troncos](#) é a abordagem moderna e preferida.

imagem dourada

Um instantâneo de um sistema ou software usado como modelo para implantar novas instâncias desse sistema ou software. Por exemplo, na manufatura, uma imagem dourada 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, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a [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 retenção

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de aprendizado [de máquina](#). Você pode usar dados de retenção para avaliar o desempenho do modelo comparando as previsões 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 típico de uma DevOps versão.

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 a [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 a [Internet das Coisas industrial](#).

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. [Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que infraestruturas mutáveis](#). Para obter mais informações, consulte as melhores práticas de [implantação usando infraestrutura imutável](#) no Well-Architected AWS 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 fabricação por meio de avanços em conectividade, dados em tempo real, automação, análise 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

Consulte [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

Consulte [a biblioteca de informações](#) de TI.

ITSM

Veja o [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](#).

modelo de linguagem grande (LLM)

Um modelo de [IA](#) de aprendizado profundo que é pré-treinado em uma grande quantidade de dados. Um LLM pode realizar várias tarefas, como responder 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 etiquetas](#).

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 [um modelo de linguagem grande](#).

ambientes inferiores

Veja o [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 a [filial](#).

malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vaziar informações confidenciais ou obter acesso não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Tróia, 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 abstratos.

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

Consulte [Migration Acceleration Program](#).

mecanismo

Um processo completo no qual 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 o [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 microsserviço 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 microsserviços 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 a Amazon EC2 com o AWS 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 o. 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 carga de trabalho para o. Nuvem AWS Para obter mais informações, consulte a entrada de [7 Rs](#) neste glossário e consulte [Mobilize sua organização para acelerar migrações em grande escala](#).

ML

Veja o [aprendizado de máquina](#).

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 [Estratégia para modernizar aplicativos no 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 [Avaliação da prontidão para modernização de aplicativos no 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](#).

MAPA

Consulte [Avaliação do portfólio de migração](#).

MQTT

Consulte 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 cargas de trabalho 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 o [controle de acesso de origem](#).

CARVALHO

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

OCM

Veja o [gerenciamento de mudanças 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 a [integração de operações](#).

OLA

Veja o [contrato em 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

Consulte [Comunicação de processo aberto — Arquitetura unificada](#).

Comunicação de processo aberto — Arquitetura unificada (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 melhores práticas 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 Well-Architected AWS Framework.

tecnologia operacional (OT)

Sistemas de hardware e software que funcionam com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas OT e de tecnologia da informação (TI) 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 a [análise de prontidão operacional](#).

OT

Veja a [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 as [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

Consulte [controlador lógico programável](#).

AMEIXA

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

política

Um objeto que pode definir permissões (consulte a [política baseada em identidade](#)), especificar as condições de acesso (consulte a [política baseada em recursos](#)) ou definir as permissões máximas para todas as contas em uma organização em AWS Organizations (consulte a 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. Para obter mais informações, consulte [Habilitar a persistência de dados em microsserviços](#).

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 WHERE cláusula.

pressão de predicados

Uma técnica de otimização de consulta 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 o desempenho 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 de engenharia de sistema 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](#) projetado para impedir a implantação de recursos não compatíveis. Esses controles examinam 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 o design, desenvolvimento e lançamento, passando pelo crescimento e maturidade, até o declínio e a remoção.

ambiente de produção

Veja o [ambiente](#).

controlador lógico programável (PLC)

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

encadeamento imediato

Usando a 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 no qual outros microsserviços possam se inscrever. 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, responsável, consultado, informado \(RACI\)](#).

RAG

Consulte [Geração Aumentada de 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, responsável, consultado, informado \(RACI\)](#).

RCAC

Veja o [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.

rearquiteta

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 mais informações, consulte [Especificar o que Regiões da AWS sua conta pode usar](#).

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.

realocar

Veja [7 Rs](#).

redefinir a plataforma

Veja [7 Rs](#).

recomprar

Veja [7 Rs](#).

resiliência

A capacidade de um aplicativo de resistir ou se recuperar de interrupções. [Alta disponibilidade](#) e [recuperação de desastres](#) são considerações comuns ao planejar a resiliência no. Nuvem AWS Para obter mais informações, consulte [Nuvem AWS Resiliência](#).

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](#).

aposentar-se

Veja [7 Rs](#).

Geração Aumentada de Recuperação (RAG)

Uma tecnologia de [IA generativa](#) na qual 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](#).

alternância

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

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 o [objetivo do ponto de recuperação](#).

RTO

Veja o [objetivo do 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 AWS Management Console 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 a [política de controle de serviços](#).

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele 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 [O que há em um segredo do Secrets Manager?](#) na documentação do Secrets Manager.

segurança por design

Uma abordagem de engenharia de sistemas que leva em conta 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 principais de controles de segurança: preventivos, detectivos, responsivos e proativos.](#)

fortalecimento 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 correção de uma instância EC2 da Amazon ou a rotação 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 medida de um aspecto de desempenho de um serviço, como taxa de erro, disponibilidade ou taxa de transferência.

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme medida 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 [informações de segurança e sistema de gerenciamento de eventos](#).

ponto único de falha (SPOF)

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

SLA

Veja o contrato [de nível de serviço](#).

ESGUIO

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

SLO

Veja o objetivo do [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 [Abordagem em fases para modernizar aplicativos no](#) Nuvem AWS

CUSPE

Veja [um único ponto de falha](#).

esquema de estrelas

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 uso 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 de supervisão 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 o desempenho. Você pode usar o [Amazon CloudWatch Synthetics](#) para criar esses testes.

prompt do sistema

Uma técnica para fornecer contexto, instruções ou diretrizes a um [LLM](#) para direcionar seu comportamento. Os prompts do sistema ajudam a definir o contexto e 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. 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 o [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 o [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 back-end.

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.

MINHOCA

Veja [escrever uma vez, ler muitas](#).

WQF

Consulte [Estrutura de qualificação AWS da carga de](#) trabalho.

escreva uma vez, leia muitas (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, geralmente malware, que tira proveito de uma vulnerabilidade de [dia zero](#).

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.

aviso zero-shot

Fornecer a um [LLM](#) instruções para realizar uma tarefa, mas sem exemplos (fotos) que possam ajudar a orientá-la. O LLM deve usar seu conhecimento pré-treinado para lidar com a tarefa. A

eficácia da solicitação zero depende da complexidade da tarefa e da qualidade da solicitação. Veja também a solicitação [de algumas fotos](#).

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.