Criação de uma estratégia de nuvem única, híbrida e multinuvem na educação

AWS Orientação prescritiva

AWS Orientação prescritiva: Criação de uma estratégia de nuvem única, híbrida e multinuvem na educação

Table of Contents

Criação de uma estratégia de nuvem única, híbrida e multinuvem na educação

Amazon Web Services (colaboradores)

Setembro de 2023 (histórico do documento)

As instituições educacionais estão buscando apoiar funções como aprendizado remoto, pesquisa, experiência estudantil, insights de dados e administração com a agilidade, economia de custos, segurança e resiliência que a computação em nuvem oferece. Muitas organizações estão avaliando as implantações híbridas e multinuvem como parte dessa transformação digital.

Este paper fornece recomendações sobre a criação de uma estratégia de governança e tecnologia de nuvem única, híbrida e multinuvem para líderes executivos e tomadores de decisão em instituições educacionais que estão avaliando suas opções de nuvem. Essa orientação é baseada em nossa experiência na AWS trabalhando com mais de 14 mil instituições educacionais de todos os tamanhos em todo o mundo, desde escolas primárias e secundárias até o ensino superior.

Visão geral do

À medida que as instituições educacionais se transformam digitalmente para oferecer serviços e experiências diferenciados a seus alunos, pais, o corpo docente, funcionários e a comunidade, elas enfrentam uma infinidade de decisões técnicas. Muitas organizações já tomaram a decisão de adotar a nuvem para aumentar a agilidade, elasticidade, resiliência, segurança e economia de custos. Com base em seus relacionamentos e investimentos existentes em várias equipes, a maioria das organizações está usando alguma combinação de data centers on-premises, instalações de colocalização e provedores de nuvem. Dada a disponibilidade de várias opções de nuvem, as instituições educacionais devem frequentemente decidir entre modelos de implantação de nuvem única, híbrida e multinuvem (definidos na seção Estratégias de implantação em nuvem).

A multinuvem, que é o uso de serviços de pelo menos dois provedores de serviços em nuvem, não é incomum para muitas instituições atualmente. Sua equipe de TI pode preferir um provedor de nuvem, enquanto outros grupos, departamentos ou usuários individuais podem escolher ou já estar usando provedores alternativos. As instituições educacionais que não têm uma estratégia clara para orientá-las para o modelo de implantação de nuvem apropriado enfrentam muitos desafios. Isso inclui complexidade desnecessária, demandas crescentes de pessoal, governança inconsistente

e abordagens de menor denominador comum que as limitam ao subconjunto de recursos básicos que são comuns a todos os provedores. Cada desafio reprime a inovação e retarda a transformação digital.

Por outro lado, se você tiver uma estratégia de nuvem que oriente você a usar uma nuvem única, híbrida e multinuvem, poderá atender aos requisitos de sua missão educacional e, ao mesmo tempo, aproveitar as vantagens da nuvem de uma forma operacionalmente sustentável para o sucesso de longo prazo. Para criar essa estratégia, recomendamos o seguinte:

- Selecione um provedor de nuvem primário e estratégico.
- Estabeleça um Centro de Excelência em Nuvem (CCoE).
- Diferencie entre aplicações de software como serviço (SaaS) e serviços básicos em nuvem.
- Estabeleça requisitos de segurança e governança para cada provedor de serviços de nuvem.
- Adote soluções gerenciadas nativas da nuvem sempre que for possível e prático.
- Implemente arquiteturas híbridas quando os investimentos on-premises existentes justificarem o uso contínuo.
- Reserve a multinuvem somente para workloads que não atendem aos requisitos técnicos ou comerciais por meio de um único provedor de nuvem.

Essas práticas recomendadas são discutidas em detalhes na seção Recomendações deste paper. Cada recomendação é importante, mas as prioridades da sua instituição dependerão do estágio de adoção da nuvem. Por exemplo, se você está apenas começando a adotar a nuvem, concentre-se em selecionar um provedor de nuvem principal e estratégico, estabelecer um CCo E e adotar soluções gerenciadas nativas da nuvem. Se você já usa um único provedor de nuvem, concentre-se em estabelecer os principais requisitos de segurança e governança, e considere arquiteturas híbridas quando seus investimentos existentes em data centers estimularem o uso contínuo. Se sua organização já usa vários provedores de nuvem, concentre-se em diferenciar as aplicações SaaS e reservar implantações multinuvem para as workloads raras que realmente precisam disso.

Índice

Estratégias de implantação de nuvem

A AWS define a computação em nuvem como a entrega sob demanda de recursos de TI pela internet com preço conforme o uso. Em vez de comprar, possuir e manter data centers e servidores físicos, você pode acessar serviços de tecnologia, como capacidade de computação, armazenamento e bancos de dados, conforme necessário, de um provedor de nuvem. A computação em nuvem permite que instituições de ensino evitem trabalhos pesados indiferenciados, como compra e manutenção de hardware e planejamento de recursos. Ao adotar e implantar soluções em nuvem, você pode escolher entre vários modelos: nuvem única, nuvem híbrida e multinuvem.

Nuvem única

Esse modelo usa apenas um único provedor de serviços em nuvem. Aplicações e workloads em uma única nuvem podem ser implementadas diretamente na nuvem, ou podem ser previamente hospedadas em outro ambiente e migradas para a nuvem. Essas workloads podem usar serviços de infraestrutura de nível inferior de seu provedor de nuvem ou também aproveitar os serviços gerenciados de nível superior. Independentemente disso, esse modelo adota um único provedor de nuvem e usa somente serviços em nuvem desse provedor.

Nuvem híbrida

Um modelo de nuvem híbrida distribui recursos no próprio data center on-premises da organização e em pelo menos um provedor de serviços em nuvem. Normalmente, o objetivo desse modelo é estender a infraestrutura de uma organização para a nuvem e, ao mesmo tempo, manter a conectividade privada com os sistemas internos existentes que residem on-premises.

Multinuvem

Um modelo multinuvem distribui recursos e usa serviços de pelo menos dois provedores de serviços em nuvem. Uma organização pode optar por ser multinuvem, mas, na maioria das vezes, isso é um resultado não intencional de equipes, departamentos ou membros da equipe individuais terem suas próprias preferências por diferentes provedores de nuvem.

Recomendações

Agora que você já tem uma compreensão básica sobre nuvem única, nuvem híbrida e multinuvem, esta seção fornece recomendações detalhadas para escolher um modelo.

- Selecionar um provedor de nuvem primário e estratégico
- Estabeleça um CCo E
- Diferenciar entre aplicações SaaS e serviços básicos em nuvem
- Estabelecer requisitos de segurança e governança para cada provedor de serviços de nuvem
- Adotar serviços gerenciados nativos da nuvem sempre que for possível e prático
- Implementar arquiteturas híbridas quando os investimentos on-premises existentes justificarem o uso contínuo
- Reservar a multinuvem somente para workloads que não podem atender aos requisitos técnicos ou comerciais por meio de um único provedor de nuvem

Selecionar um provedor de nuvem primário e estratégico

A adoção da nuvem oferece uma ampla gama de vantagens que são essenciais para a modernização, a eficácia de custos e a inovação da TI. No entanto, a adoção de tecnologias de nuvem além das aplicações SaaS limitadas pode apresentar desafios que as instituições educacionais devem planejar cuidadosamente para evitar custos e complexidades desnecessários. As mudanças tecnológicas e comerciais envolvidas na implementação de workloads na nuvem exigem a capacitação da equipe e ajustes na infraestrutura principal, incluindo rede, segurança, governança e operações.

A melhor abordagem para enfrentar esses desafios de forma eficaz, especialmente se sua organização estiver nas etapas iniciais de sua jornada para a nuvem, é selecionar um provedor de nuvem primário e estratégico para ser compatível maioria de suas workloads. Comece com uma adoção focada e centrada nesse provedor para que você possa simplificar e acelerar a obtenção das vantagens da nuvem. A seleção de um provedor de nuvem primário não é uma decisão exclusiva e irreversível. Ela permite que sua organização desenvolva sua adoção da nuvem de forma iterativa. Você pode começar concentrando-se em alguns serviços e depois expandir para outros serviços de nuvem, conforme e onde necessário, sem retardar as vantagens gerais da nuvem. Essa abordagem maximiza a capacidade da sua organização de aproveitar os recursos de um provedor, concentrar

e desenvolver as habilidades dos funcionários e os relacionamentos com parceiros terceiros e simplificar o gerenciamento de fornecedores.

Já vimos clientes embarcarem em sua jornada para a nuvem tentando adotar simultaneamente vários provedores de nuvem, mas depois se arrependeram dessa decisão e da complexidade que ela gerou. O Gartner compartilha esse insight em seu artigo, 6 Steps for Planning a Cloud Strategy, em que a etapa 2 é “Priorizar um provedor primário em arquiteturas multinuvem”.

Cada provedor de nuvem apresenta diferentes modelos operacionais e de suporte, gerenciamento de identidades e acesso, redes, operações, recursos de conformidade e muito mais. É melhor dominar o modelo operacional de um provedor de nuvem por vez.Depois, você pode incorporar serviços de nuvem adicionais de forma iterativa e incremental, quando racionalizados. Muitos fatores podem influenciar sua decisão de adotar um provedor de nuvem primário, mas use as seguintes perguntas-chave para orientar sua escolha.

- Qual é a abrangência e a profundidade dos serviços oferecidos pelo provedor?

  Diferentes provedores de nuvem oferecem serviços diversos. No mínimo, certifique-se de que seu provedor primário tenha os recursos necessários para suportar todos os seus requisitos funcionais, bem como suas necessidades operacionais transversais, como segurança, governança e automação. Selecione um fornecedor que ofereça esses recursos com um histórico comprovado de inovação e excelência operacional. Considere não apenas suas aplicações, mas também seus dados. Pense nos padrões futuros de integração e transferência de dados para limitar o custo, a latência e a complexidade da movimentação de grandes quantidades de dados entre provedores. Escolha um provedor que tenha a maior abrangência e profundidade possíveis de serviços para satisfazer suas necessidades atuais de aplicações e dados, e também para desbloquear novos casos de uso que possam atender às necessidades da sua instituição à medida que elas mudam com o tempo.
- O provedor pode atender a todas as suas necessidades de segurança e conformidade?

  Na educação, a segurança e a conformidade são essenciais para qualquer implantação de tecnologia. Escolha um provedor de nuvem que seja capaz de atender a todas as suas necessidades de segurança e conformidade. Ferramentas como o AWS Artifact podem ajudar você a avaliar os provedores, oferecendo um recurso central para acesso sob demanda a relatórios de segurança e conformidade. Considere não apenas a segurança e a conformidade da infraestrutura e dos serviços do próprio provedor de nuvem, mas também a facilidade para arquitetar soluções seguras e compatíveis usando esses serviços. Prefira um provedor que

ofereça alguma combinação de soluções pré-criadas, inícios rápidos e recomendações para acelerar sua adoção segura da nuvem.

- O provedor tem uma rede de parceiros robusta?

  Nenhuma organização passa pela transformação da nuvem sozinha. Para acelerar a adoção, você deve usar os serviços e a experiência do provedor de nuvem, bem como de sua rede de parceiros. Essa rede inclui parceiros de tecnologia que fornecem software executado, integrado ou compatível com a tecnologia de nuvem, bem como parceiros de consultoria que podem ajudar você a projetar, criar, executar e gerenciar suas próprias aplicações na nuvem. Você descobrirá que muitos provedores de tecnologia educacional, fornecedores independentes de software (ISVs), consultores e revendedores com os quais você já trabalha são membros da rede de parceiros do provedor de nuvem. Prefira um provedor de nuvem que tenha a rede mais robusta de parceiros com competências comprovadas. Ter parceiros com experiência técnica e setorial comprovada é fundamental.

- Que suporte e capacitação o provedor oferece?

  Para adotar com êxito qualquer nova tecnologia, você precisa de mecanismos para solicitar treinamento e ajuda, incluindo recomendações de práticas recomendadas, orientação de configuração e resolução de problemas de correção de falhas. Escolher um provedor de nuvem que ofereça opções sólidas de suporte e treinamento preparará você para o sucesso. Analise o modelo e os recursos de suporte oficiais do provedor, bem como quaisquer recursos disponíveis de terceiros ou baseados na comunidade, como blogs, fóruns, vídeos e guias de instruções. Considere não apenas os programas de suporte técnico do provedor, mas também os programas que se concentram na transformação comercial e cultural. Por exemplo, o AWS Cloud Adoption Framework (AWS CAF) ajuda as organizações a se transformarem digitalmente, concentrando-se em perspectivas que incluem processos e pessoas de negócios, não apenas tecnologia. Prefira um provedor de nuvem que ofereça uma ampla gama de opções de treinamento e uma comunidade e um modelo de suporte comprovados e confiáveis.

Estabeleça um CCo E

Considere desenvolver sua função de liderança na nuvem por meio de um escritório de transformação ou de um Centro de Excelência em Nuvem (CCoE). A CCo E desenvolve e evangeliza uma abordagem para implementar a tecnologia de nuvem em grande escala em toda a organização. Para uma adoção bem-sucedida da nuvem, projete seu CCo E para incluir representantes que possam falar pelas equipes e departamentos envolvidos. Comece aos poucos e evolua

gradualmente o CCo E para atender às suas necessidades à medida que avança na jornada de transformação. Seus representantes principais do provedor de nuvem, como seu gerente de AWS contas e arquiteto de soluções, podem fornecer recursos para orientá-lo na criação do seu CCo E. A CCo E acelera sua capacidade de estabelecer experiência no assunto, obter adesão, ganhar confiança em toda a organização e estabelecer diretrizes eficazes para atender aos requisitos de sua missão. Não existe uma estrutura organizacional única que funcione para todas as instituições, mas as perguntas a seguir ajudarão você a criar seu próprio CCo E.

- Quem você deve incluir no seu CCo E?

  No início, um CCo E pode incluir apenas alguns pioneiros e campeões da nuvem. O CCo E pode continuar pequeno, mas deve evoluir para incluir campeões que possam falar tanto pelas funções comerciais quanto pelas funções técnicas afetadas pela adoção da nuvem. As funções de negócios incluem gerenciamento de mudanças, requisitos das partes interessadas, governança, treinamento, aquisição e comunicações. Essas funções geralmente são representadas por membros das equipes administrativas e instrucionais da sua instituição. As funções técnicas incluem infraestrutura, automação, ferramentas operacionais, segurança, performance e disponibilidade. Essas funções geralmente são representadas por membros das equipes de TI da sua instituição. A CCo E também deve procurar envolver fornecedores e parceiros, conforme necessário, para fornecer experiência no assunto. A CCo E é uma organização viva. Sua filiação, forma e função provavelmente mudarão com o tempo e poderão até mesmo se dissolver em algum momento de maturidade futura.
- Como a CCo E interage com suas partes interessadas?

  O CCo E está a serviço de outras equipes e tem como objetivo apenas informar e permitir a adoção bem-sucedida da nuvem. Veja a incorporação de partes do CCo E em vários departamentos, escolas e funções. Isso permite o acesso a uma maior gama de recursos e um feedback interno mais rápido. Concentre-se na criação de parcerias e linhas abertas de comunicação entre as partes interessadas desde o início para estabelecer confiança dentro da instituição e eliminar os silos organizacionais. O CCo E deveria ter definido mecanismos para se comunicar com as partes interessadas, coletar feedback e treinar usuários. As métricas de sucesso do CCo E devem refletir essa colaboração e comunicação. Se uma equipe for avaliada apenas com relação à criação de tecnologia, mais tecnologia será criada, mas seu uso e resultados se tornarão secundários. Em vez disso, suas métricas devem medir coisas como o número de equipes que se tornam autossuficientes por meio do trabalho do CCo E, o número de vezes que o CCo E está no caminho crítico para as iniciativas, o número de eventos de treinamento realizados ou a amplitude da adoção dos resultados do CCo E. Um E bem construído

CCo e confiável pode ser um trampolim para uma transformação organizacional maior baseada na confiança.

- Como você deve estabelecer um CCo E?

  A maioria das organizações inicia a adoção da nuvem com projetos piloto específicos e direcionados. Estabeleça um CCo E como parte desses projetos. Um bom começo é fundamental para definir o sucesso de toda a jornada.

  - Comece com um problema de negócio. A tecnologia em prol da tecnologia é uma estratégia ruim. Se você estiver experimentando tecnologias de nuvem, identifique um caso de uso de negócio convincente, por menor que pareça. Em seguida, retroceda a partir desse caso de uso para definir metas claras sobre como a tecnologia pode ajudar. Não implemente a solução em um silo. Receba contribuições constantes das partes interessadas da empresa antes e durante a implementação do projeto. Todos os projetos de nuvem bem-sucedidos dependem da estreita colaboração com as unidades institucionais que usarão a tecnologia.
  - Comece pequeno. Escolha um projeto de baixo risco que ofereça uma porta bidirecional. Isso significa que o projeto é reversível e qualquer erro pode ser corrigido rapidamente. Os projetos piloto se resumem à experimentação. Evitar projetos de grande escala e de alto risco oferece melhor controle sobre a implementação e os resultados. Isso ajuda a direcionar problemas específicos e bem definidos em vez de metas abrangentes. Por exemplo, se a automação for a meta final, tente automatizar tarefas específicas em vez de trabalhos inteiros.
  - Defina e avalie o resultado. Defina métricas claras para avaliar o progresso e a performance de cada projeto. Defina o estado final desejado com bastante antecedência para evitar expectativas incompatíveis entre as partes interessadas. Trabalhe em estreita colaboração com as partes interessadas do negócio e outros líderes da organização para definir expectativas e ganhos mensuráveis. Também é importante comunicar os resultados em uma linguagem não técnica. Fale em termos de metas institucionais, como a forma como o projeto melhorou a retenção e reduziu a rotatividade, como reduziu os custos e aumentou a velocidade de entrega etc.
  - Comece na zona de conforto. Escolha um projeto dentro de um domínio com o qual sua instituição esteja familiarizada. Dessa forma, você pode garantir que o projeto tenha metas significativas e compreensíveis com impacto real. Esse projeto criará confiança e terá melhores resultados no longo prazo para sua organização. Por exemplo, caso já tenha conhecimento especializado em data analytics, você pode iniciar sua jornada para a nuvem e, ao mesmo tempo, aproveitar suas competências atuais começando com um projeto de analytics. Cada instituição tem diferentes conhecimentos especializados e precisa encontrar seus componentes exclusivos para criar uma estratégia de transformação digital bem-sucedida.

Diferenciar entre aplicações SaaS e serviços básicos em nuvem

A maioria das instituições educacionais já adotou aplicações de software como serviço (SaaS). O SaaS fornece à sua instituição uma solução completa que é executada e gerenciada pelo provedor de serviços. As aplicações SaaS comuns incluem aplicações de produtividade, como processamento de texto e e-mail, mas também existem opções de SaaS para muitas workloads essenciais, como planejamento de recursos corporativos (ERP), sistemas de informações estudantis (SIS) e sistemas de gerenciamento de aprendizado (LMS). Quando sua instituição adota uma oferta de SaaS, sua equipe de TI não precisa se preocupar em como o serviço é mantido ou como a infraestrutura é gerenciada. Seus usuários simplesmente consomem o serviço. Esse modelo de entrega reduz a carga de gerenciamento de sua equipe de TI. Muitas instituições optam por adotar uma abordagem “SaaS em primeiro lugar” em sua estratégia de TI, especialmente se suas equipes de TI não tiverem tempo, recursos ou as competências necessárias para ter capacidade de hospedar a própria aplicação. Mesmo que você tenha os recursos para auto-hospedagem, ainda pode ser mais econômico adotar uma solução SaaS e investir em outros projetos.

Quando você usa aplicações SaaS, sua equipe de TI não precisa gerenciar a infraestrutura subjacente, portanto, o local onde o provedor hospeda a aplicação (data center on-premises, seu provedor de nuvem primário ou um provedor de nuvem alternativo) se torna algo secundário. Depois de escolher um provedor de nuvem primário e estratégico, você pode optar por usar uma oferta de SaaS hospedada em outro provedor de nuvem ou on-premises, no data center do provedor. Por outro lado, mesmo que suas aplicações SaaS estejam hospedadas em um provedor de nuvem, você pode escolher outro provedor de nuvem primário e estratégico com base na capacidade dele para suas workloads não SaaS. A distinção entre ambientes de hospedagem é menos importante para SaaS do que para aplicações auto-hospedadas. No entanto, você ainda deve considerar as questões-chave a seguir ao avaliar como o SaaS se encaixa na nuvem como parte de sua estratégia de TI.

- A aplicação SaaS é altamente disponível e escalável?

  Muitos provedores já tomaram a decisão de adotar a nuvem para suas ofertas de SaaS. Ao fazer isso, o provedor é capaz de obter as vantagens da nuvem de maior disponibilidade e escalabilidade. Além disso, como o provedor pode adotar o modelo de responsabilidade compartilhada da nuvem em vez de gerenciar e manter a infraestrutura física, ele pode investir mais tempo e recursos na entrega de novos recursos. Por causa desses benefícios, você deve dar preferência a provedores que priorizem a nuvem e ofereçam soluções hospedadas na nuvem.
- A aplicação SaaS pode atender aos seus requisitos de segurança?

Ao avaliar o SaaS, é importante saber quais dados a aplicação armazena, como esses dados são usados e quais controles de segurança existem para proteger esses dados. Embora você possa não ter controle direto sobre o armazenamento de dados como teria em seu próprio ambiente auto-hospedado, você deve se certificar de que o provedor tenha mecanismos e controles para lidar com seus dados de forma adequada. Esteja ciente de quais recursos de segurança estão incorporados à solução SaaS e quais recursos exigem configuração adicional. A nuvem permite que os provedores de SaaS criem soluções mais disponíveis e escaláveis, e que também possam criar soluções mais seguras por causa do modelo de responsabilidade compartilhada. Você deve dar preferência aos fornecedores que incorporam as ferramentas e os serviços de segurança na nuvem como parte de suas soluções.

- Quem é o proprietário dos dados da aplicação SaaS e como você pode acessá-los?

  Ao usar o SaaS, você confia no provedor para lidar adequadamente com os dados da sua instituição. Certifique-se de revisar os termos e os acordos de serviço para aplicações SaaS para entender os fatores que contribuem, como propriedade, disponibilidade e durabilidade dos dados. Avalie os mecanismos para fazer backup ou exportar seus dados. Eles são especialmente importantes caso você decida mudar de provedor ou o provedor descontinue o serviço.

- Seus outros serviços e aplicações auto-hospedadas podem se integrar à aplicação SaaS, independentemente do ambiente?

  Ao adotar uma solução SaaS, é fácil supor que os serviços e as aplicações que compartilham o mesmo ambiente de hospedagem (ou seja, aplicações que usam o mesmo provedor de nuvem ou o data center do mesmo fornecedor) terão uma integração mais otimizada. No entanto, a maioria das soluções SaaS atuais oferece amplo suporte para integrações via API e com terceiros, portanto, não se limite a soluções hospedadas no mesmo ambiente. Se as integrações necessárias existirem, as soluções não precisarão compartilhar o mesmo ambiente subjacente. Por exemplo, digamos que você esteja usando uma solução SaaS, como o Google Drive ou a Microsoft, OneDrive para armazenamento de arquivos de estudantes na nuvem. Para fornecer desktops virtuais e streaming de aplicativos para seus alunos, você pode determinar que o Amazon WorkSpaces Applications é o mais adequado às suas necessidades. Embora esses serviços sejam executados em ambientes diferentes, o WorkSpaces Applications tem integrações nativas com o Google Drive e a Microsoft OneDrive, para que seus alunos possam continuar usando o armazenamento existente.

- A aplicação SaaS oferece suporte ao gerenciamento centralizado de identidades?

Para evitar que sua equipe de TI tenha que gerenciar diferentes repositórios de identidades e que seus usuários tenham que se lembrar de vários conjuntos de credenciais, certifique-se de que suas soluções SaaS ofereçam suporte à integração com suas soluções existentes de gerenciamento de identidades ou de autenticação única. O gerenciamento fragmentado de identidades diminui a produtividade e pode levar a práticas de segurança inadequadas, como aumento de privilégios e senhas fracas. Se a solução SaaS desejada não oferecer suporte à autenticação única ou ao seu repositório de identidades atual, avalie se o valor comercial da adoção da solução supera o aumento da carga sobre os usuários e a equipe.

- Como você pode proteger a comunicação de rede com a aplicação SaaS?

  Em alguns casos, pode ser necessária uma aplicação auto-hospedada para se comunicar com uma aplicação SaaS. Normalmente, essa comunicação será feita por meio APIs de mecanismos de autenticação e autorização apropriados. No entanto, dependendo dos ambientes de hospedagem das duas aplicações, os mecanismos alternativos ou adicionais podem ser necessários para simplificar ou proteger essa comunicação. Por exemplo, se você auto-hospeda uma aplicação com um provedor de nuvem e precisa integrá-la a uma aplicação SaaS hospedada no mesmo provedor de nuvem, o provedor pode fornecer várias opções de conexão. Talvez você consiga usar conexões de emparelhamento específicas da nuvem, interfaces privadas ou privadas APIs, AWS PrivateLinkpara impedir que essa comunicação atravesse a Internet pública. Da mesma forma, se sua aplicação on-premises tiver uma conexão de rede dedicada com um provedor de nuvem por meio de um serviço como o AWS Direct Connect, você poderá usar essa mesma conexão para se comunicar com aplicações SaaS hospedadas no mesmo provedor de nuvem.

Estabelecer requisitos de segurança e governança para cada provedor de serviços de nuvem

As entidades educacionais precisam atingir diversos objetivos relacionados à conformidade regulatória, à governança e à segurança cibernética. Os riscos de não cumprir esses objetivos podem incluir perda de reputação institucional, multas financeiras, resgates, violações de dados sensíveis, roubo de propriedade intelectual e perda degradada ou total de funções essenciais. Por causa do modelo de responsabilidade compartilhada, as instituições que adotam serviços em nuvem podem reduzir a carga administrativa transferindo parte da responsabilidade pela segurança da infraestrutura para o provedor de serviços em nuvem. Além disso, você pode se beneficiar de serviços de segurança projetados especificamente e nativos da nuvem que oferecem recursos que

geralmente não estão disponíveis, são difíceis de gerenciar ou têm um custo proibitivo em uma implantação on-premises. Os exemplos incluem serviços como proteção AWS WAFde aplicativos web, AWS Shieldproteção distribuída de negação de serviço (DDoS) e Amazon GuardDuty para detecção de ameaças. Uma estratégia bem-sucedida de segurança e governança na nuvem permite que as equipes de TI e segurança se concentrem na criação de sistemas que sejam seguros por design, ajuda a instituição a se adaptar rapidamente aos requisitos de missão em evolução e fornece ao corpo docente e aos pesquisadores ambientes seguros para aprendizado e inovações de ponta. Para avaliar seus requisitos de segurança e governança, considere as seguintes perguntas-chave.

- A quais frameworks de conformidade suas workloads devem se alinhar?

  As instituições educacionais devem aderir a muitos frameworks de conformidade devido à multiplicidade de partes interessadas e de workloads que elas gerenciam. Esses frameworks de conformidade incluem a Lei de Privacidade e Direitos Educacionais da Família (FERPA), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA), o Programa Federal de Gerenciamento de Riscos e Autorizações (FedRAMP), a Certificação do Modelo de Maturidade em Segurança Cibernética (CMMC), o Regulamento Internacional de Tráfego de Armas (ITAR), os Serviços de Informações da Justiça Criminal (CJIS) e o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS). Em alguns casos, como no CMMC, o financiamento da bolsa de pesquisa não é liberado até que as workloads relevantes sejam certificadas como compatíveis. Cada framework é exclusivo e pode ser aplicado somente a um subconjunto de workloads. Certifique-se de saber quais workloads devem aderir a quais requisitos e de que você é capaz de atender a esses requisitos no ambiente de cada workload. Em ambientes de nuvem, certifique-se de entender suas responsabilidades em comparação com as responsabilidades do provedor de nuvem. Você deve ter o conhecimento, os recursos e as competências necessários para alcançar e manter a conformidade.
- Quais mecanismos você tem para impor a conformidade em vários provedores de nuvem sem inibir a inovação?

  Se sua instituição acadêmica for nova na nuvem, recomendamos que você selecione um provedor estratégico primário de serviços de nuvem e se concentre em entender como arquitetar, projetar e operar ambientes de nuvem que sejam seguros por design. De preferência, os controles de segurança que são incorporados automaticamente aos sistemas de autoatendimento permitem que os usuários implantem rapidamente ambientes de nuvem seguros com uma quantidade mínima de intervenção das equipes de TI. Concentrar-se em um único provedor limita a quantidade de recursos e o tempo que você deve investir para garantir a segurança e a conformidade. As instituições mais bem-sucedidas selecionam um provedor de serviços em

nuvem que possa atender à maioria dos requisitos de conformidade, tenha uma rede robusta de parceiros, ofereça soluções de conformidade pré-criadas e disponibilize a automação segura de autoatendimento. Se você precisar garantir a segurança e a conformidade em vários provedores de nuvem, será necessário um investimento adicional para criar as capacidades e os recursos para gerenciar a conformidade em cada ambiente. Se cada provedor de nuvem usar um ambiente básico ou zona de pouso diferente, você precisará entender para quais padrões e requisitos de conformidade cada zona de pouso oferece suporte, e isso pode determinar se certas workloads podem ser hospedadas nesse provedor. Você pode gerenciar a conformidade de cada provedor separadamente ou usar soluções personalizadas ou de parceiros que possam centralizar o gerenciamento entre os provedores. O AWS Marketplace fornece soluções turnkey que também podem atender aos seus requisitos de conformidade.

- Como você pode avaliar e controlar o custo e o uso em vários provedores de nuvem?

  Se sua instituição acadêmica for nova na nuvem, recomendamos que você estabeleça mecanismos de controle e visibilidade de custos para obter insights sobre quais serviços de nuvem estão sendo usados, a quem pertencem os recursos de nuvem, qual é a finalidade desses recursos e quais possíveis economias de custo podem ser obtidas com a otimização do consumo. As instituições podem obter um retorno significativo sobre o investimento em parceria com seu provedor de serviços de nuvem para migrar e modernizar sistemas de missão crítica, pois podem negociar acordos corporativos, beneficiar-se dos preços por volume e aproveitar a experiência do provedor de serviços em nuvem. Se você precisar controlar o custo e o uso em vários fornecedores, considere como você pode agregar e analisar o custo e o uso de cada provedor, seja com processos e ferramentas internos ou usando soluções de parceiros. Muitas organizações estão começando a identificar as operações financeiras na nuvem (FinOps) como uma função fundamental e dedicando recursos para evangelizar e implementar recursos para gerenciamento e otimização de custos na nuvem.
- Você tem mecanismos para gerenciar facilmente as permissões dos usuários ao longo do tempo?

  Recomendamos que as instituições acadêmicas entendam as principais necessidades das partes interessadas quando abordarem a nuvem pela primeira vez. Os usuários de sistemas institucionais incluem estudantes, corpo docente, pesquisadores, equipe de TI, administração, segurança, público em geral e colaboradores terceiros. Você deve identificar as principais necessidades desses usuários e garantir que tenha mecanismos adequados para conceder a eles acesso aos serviços em nuvem. Diferentes tipos de usuários exigem diferentes tipos de acesso aos serviços em nuvem. Por exemplo, estudantes, o corpo docente e o público em geral precisam acessar as aplicações; a equipe de TI, os administradores e a segurança precisam acessar a

infraestrutura de nuvem; os pesquisadores e seus colaboradores terceiros precisam acessar ambientes de pesquisa seguros; o corpo docente precisa acessar ambientes de ensino seguros e talvez até queira oferecer aos alunos acesso prático às tecnologias de nuvem. Você deve ter ferramentas para gerenciar de forma centralizada e automatizada essas identidades e usar processos estabelecidos para identificar, conceder e revogar permissões à medida que as funções e responsabilidades mudam com o tempo.

- Você tem mecanismos para integrar adequadamente novos sistemas à sua solução de gerenciamento de identidades?

  Recomendamos que as instituições acadêmicas facilitem a integração de novos sistemas com seus sistemas de gerenciamento de identidades. Isso proporciona à instituição a flexibilidade para apoiar diversas funções críticas, permitindo que as partes interessadas adquiram e criem sistemas que possam ser facilmente integrados ao sistema de gerenciamento de identidades. Ao simplificar o processo de integração, as partes interessadas terão menos probabilidade de usar suas próprias medidas de controle de acesso, que podem não impor as práticas recomendadas de segurança, como autenticação única, chaves de acesso e autenticação multifator (MFA). Certifique-se de que seu sistema de gerenciamento de identidades possa interoperar com os sistemas necessários por meio de integrações nativas ou protocolos padrão do setor.
- Você tem mecanismos para permitir a detecção e a resposta eficazes a incidentes?

  As instituições educacionais são frequentemente alvo de ataques cibernéticos e ransomware. Para ajudar a detectar e responder a esses incidentes de forma eficaz, recomendamos uma abordagem bifurcada:

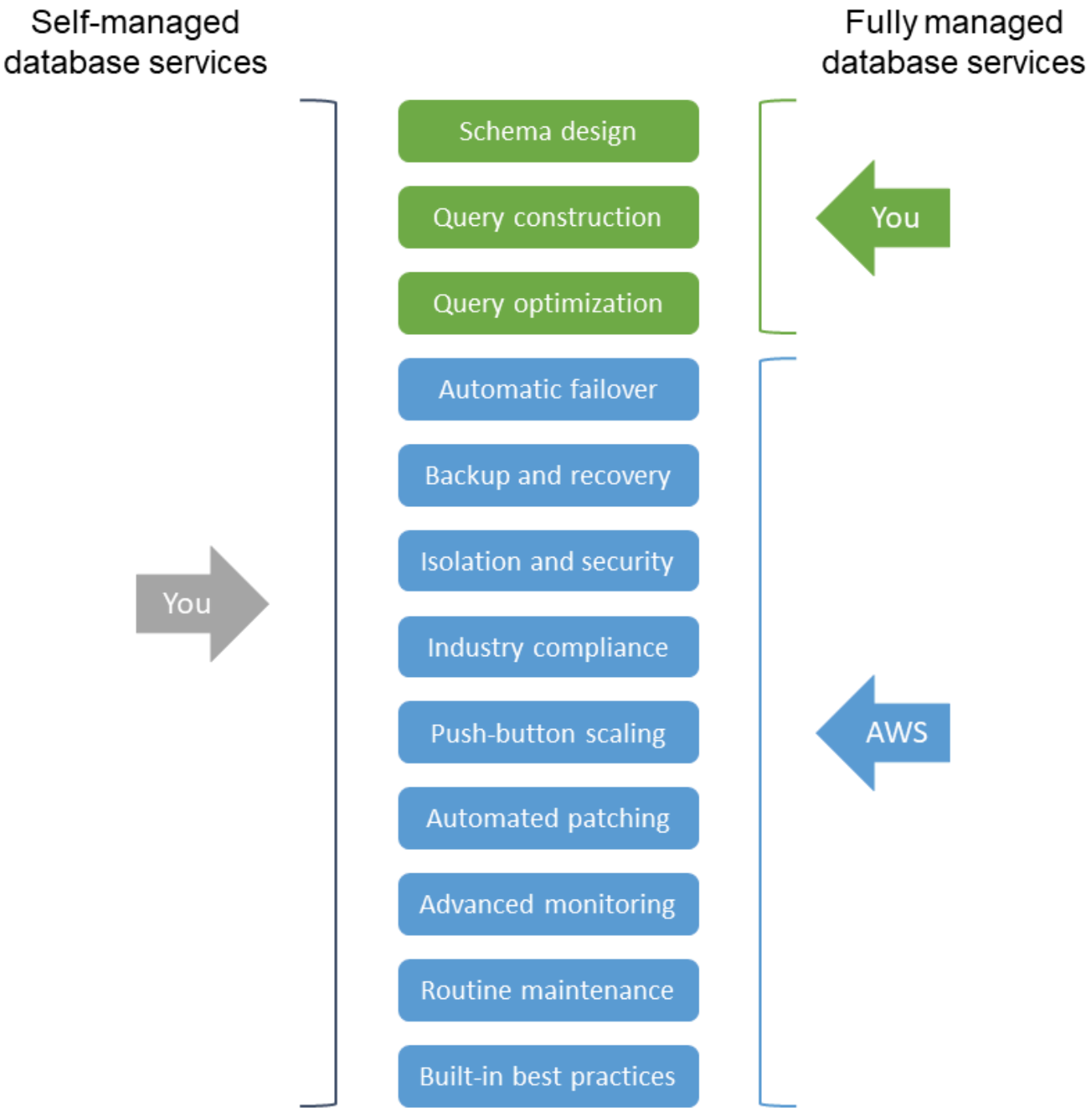
  - Concentre seus esforços em medidas preventivas na forma de controles de segurança que são incorporados automaticamente em ambientes de nuvem.
  - Implemente recursos de detecção que ajudem as equipes de resposta a incidentes cibernéticos a detectar, conter e mitigar violações de segurança em tempo hábil.

Assim como acontece com a conformidade, você deve garantir que tenha os recursos, as capacidades e as ferramentas para detectar, prevenir e responder aos eventos em cada ambiente. Ao se concentrar em um único provedor de nuvem primário, você pode limitar os recursos necessários. Instituições acadêmicas que não têm uma equipe madura de operações de segurança devem procurar provedores de software independente, provedores de detecção e resposta gerenciadas e consultores de segurança cibernética para obter ajuda nessas áreas.

Adotar serviços gerenciados nativos da nuvem sempre que for possível e prático

Quando você pensa inicialmente em como aproveitar os serviços em nuvem, usar serviços de infraestrutura e ferramentas de desenvolvimento com os quais suas equipes estão familiarizadas pode parecer o melhor caminho a seguir. No entanto, selecionar serviços gerenciados nativos da nuvem, especialmente opções com tecnologia sem servidor, pode reduzir muito o custo, o esforço e a complexidade.

Os serviços gerenciados nativos da nuvem eliminam muitas das tarefas indiferenciadas de TI que exigem tempo e esforço de sua equipe e que poderiam ser melhor gastos em atividades focadas na missão. Além disso, à medida que os provedores aprimoram os recursos de seus serviços, suas soluções naturalmente herdam melhorias incrementais em eficiência, segurança, resiliência, performance e outras características. Por exemplo, um serviço de banco de dados totalmente gerenciado é um sistema de gerenciamento de banco de dados relacional completo, mas você não precisa provisionar nem gerenciar o servidor e o sistema operacional subjacentes em que o banco de dados é executado. Isso elimina as tarefas administrativas que normalmente são necessárias quando você mantém um banco de dados relacional em seu próprio data center ou em um servidor virtual autogerenciado que você provisiona na nuvem. O diagrama a seguir ilustra essa diferença.



As vantagens de eliminar o gerenciamento da infraestrutura ficam claros quando você compara qualquer serviço gerenciado nativo da nuvem com uma abordagem autogerenciada comparável. Como resultado, sempre que precisar implantar componentes em que suas aplicações adquiridas ou desenvolvidas de forma personalizada serão executadas, você deve usar serviços gerenciados nativos da nuvem para reduzir o tempo e o esforço.

Quando sua equipe for responsável por criar, implantar ou gerenciar soluções na nuvem, use serviços gerenciados nativos da nuvem para aproveitar ao máximo os recursos e as inovações diferenciadas do seu provedor de nuvem. Essa estratégia permite selecionar, integrar e implantar serviços em nuvem de forma a reduzir o tempo e o esforço que esses projetos exigem, ao mesmo tempo em que aumenta sua resiliência e segurança. Para uma estratégia de nuvem bem-sucedida, considere adotar os blocos de criação nativos da nuvem ao migrar soluções personalizadas para a nuvem, desenvolver novas soluções na nuvem ou implantar software licenciado na nuvem. Ao avaliar as opções de serviços gerenciados nativos da nuvem, considere as seguintes perguntas-chave.

- Você precisa concentrar mais tempo e esforço de sua equipe na funcionalidade que é essencial para sua missão educacional?

  O gerenciamento de servidores, mesmo os virtuais, exige tempo e atenção para garantir que eles permaneçam atualizados com atualizações e patches do software do sistema. O uso de serviços gerenciados que lidam com essas tarefas para você permite que você direcione o tempo da equipe de TI para as atividades que estejam alinhadas mais diretamente à missão da sua instituição. Por exemplo, se você precisar implantar contêineres, considere um serviço gerenciado sem servidor, como o AWS Fargate, para que você não precise configurar e manter servidores. Ao eliminar a necessidade de adquirir, provisionar e gerenciar a infraestrutura subjacente, você pode se concentrar em oferecer novas funcionalidades, otimizar a performance e melhorar a experiência do usuário. Considere esse benefício ao avaliar os serviços gerenciados em relação às opções autogerenciadas.
- Que esforço será necessário para que sua equipe adote serviços gerenciados nativos da nuvem?

  Pode haver uma curva de aprendizado para projetar e implementar soluções com serviços gerenciados nativos da nuvem, mas esses esforços serão recompensados com reduções de custo, tempo e complexidade ao longo da vida útil de uma solução. Devido à pay-as-you-go natureza sob demanda da computação em nuvem, os serviços nativos em nuvem permitem que você itere e experimente rapidamente de forma mais ágil, evitando investimentos iniciais. Isso leva a uma maior inovação e a prazos de projeto mais curtos. No entanto, para obter esses benefícios de forma eficaz, considere o que pode ser necessário para adotar e usar o serviço, como treinamento da equipe sobre padrões de uso ideais e refatoração de código para acomodar serviços específicos. APIs Mesmo que o serviço use código aberto ou padrão do setor APIs, talvez seja necessário refatorar ou configurar seu aplicativo para lidar com disparidades de recursos ou incompatibilidades de versões.
- Como você implementa e gerencia a infraestrutura atualmente? Você precisa manter esse nível de controle?

Há várias maneiras de hospedar e gerenciar a infraestrutura na nuvem, incluindo o uso de hosts bare-metal, máquinas virtuais, serviços gerenciados de contêineres e ofertas de tecnologia sem servidor. Mesmo se você estiver usando atualmente uma infraestrutura semelhante, como máquinas virtuais ou contêineres, em seu ambiente on-premises, considere se uma abordagem alternativa seria adequada para determinadas workloads. Por exemplo, em vez de executar todas as aplicações em máquinas virtuais, considere colocá-las em contêineres e aproveitar os serviços gerenciados de contêineres, como o Amazon Elastic Container Service (Amazon ECS). Isso pode exigir refatoração, mas você pode usar uma ferramenta como o AWS App2Container para simplificar e auxiliar na conteinerização. Levando isso um passo adiante, em vez de implantar servidores ou contêineres para todos os componentes, considere opções inteiramente sem servidor. As tecnologias sem servidor apresentam escalabilidade automática, alta disponibilidade integrada e um modelo de pay-for-use cobrança para aumentar a agilidade e otimizar os custos. Ao mesmo tempo, elas eliminam a necessidade de gerenciar servidores e planejar a capacidade. Serviços de computação sem servidor, como o AWS Lambda, são essenciais para arquiteturas sem servidor. O Lambda oferece suporte a linguagens de programação comuns e permite que os desenvolvedores se concentrem no código da aplicação em vez de no gerenciamento da infraestrutura. Analise essas opções para cada workload e considere fatores como curva de aprendizado, despesas gerais de gerenciamento, custo e licenciamento.

- Você precisa implantar e gerenciar a infraestrutura de qualquer software licenciado?

  Quando você implanta e gerencia software licenciado de fornecedores de software independentes (ISVs), pode parecer lógico imitar sua implantação local com a infraestrutura em nuvem. Por exemplo, você pode considerar a substituição de máquinas virtuais on-premises por máquinas virtuais hospedadas na nuvem. Embora esta seja uma opção viável, considere se você pode substituir qualquer componente da arquitetura por serviços gerenciados nativos da nuvem. Por exemplo, você pode substituir um servidor de banco de dados autogerenciado por um serviço de banco de dados totalmente gerenciado que reduza a carga administrativa ao executar o mesmo mecanismo de banco de dados. Muitos ISVs já usam arquiteturas de nuvem que aproveitam os serviços gerenciados e podem até oferecer modelos pré-criados para simplificar a implantação. Sempre ISVs que possível, você deve preferir oferecer orientação prescritiva e suporte para implantações na nuvem. Antes de implantar o software licenciado na nuvem, consulte seu ISV para entender como o licenciamento do ambiente de nuvem pode ser diferente do licenciamento on-premises.
- Você está preocupado com o fato de que o uso de um serviço gerenciado possa resultar em dependência de fornecedor?

Muitos serviços gerenciados nativos da nuvem são criados para dar suporte aos padrões comuns do setor e. APIs Por exemplo, serviços de análise como o Amazon EMR são baseados em estruturas de processamento AWS Gluee armazenamento padrão do setor, como o Apache Spark e o Apache Parquet. AWS Lambdaoferece suporte nativo aos códigos Java, Go, Microsoft PowerShell, Node.js, C#, Python e Ruby. O Amazon Relational Database Service (Amazon RDS) é compatível com várias versões de mecanismos de banco de dados comuns, incluindo SQL Server, Oracle, PostgreSQL e MySQL. Quando os serviços têm soluções proprietárias APIs, nativas ou de parceiros, podem estar disponíveis para interagir com eles APIs usando protocolos comuns e independentes da nuvem. Por exemplo, o Amazon Simple Storage Service (Amazon S3) tem uma API específica do serviço para integração direta, mas você também pode interagir com ela usando protocolos de armazenamento padrão, como Network File System (NFS), Server Message Block (SMB) e Internet Small Computer Systems Interface (iSCSI), ao usar o AWS Storage Gateway. Você ainda deve se concentrar em escolher o serviço gerenciado nativo da nuvem que melhor atenda às suas necessidades e, ao mesmo tempo, reduza ao máximo a sobrecarga operacional, mas talvez prefira serviços que usem ou disponibilizem padrões e protocolos comuns do setor.

Implementar arquiteturas híbridas quando os investimentos on-premises existentes justificarem o uso contínuo

A maioria das instituições educacionais investiu em data centers on-premises de escala variável para hospedar aplicações corporativas, soluções de armazenamento de dados, ambientes de computação de usuário final (EUC) e recursos de computação compartilhada. Todos os recursos desses data centers estão sujeitos a diferentes ciclos de atualização, em que você deve considerar o crescimento futuro e provisionar capacidade suficiente para acomodar a escala máxima, o que pode ser necessário apenas algumas vezes por ano. Como resultado, os recursos geralmente ficam ociosos até o próximo ciclo de atualização. Planejar, orçamentar, adquirir e implantar um novo hardware pode levar semanas, se não meses ou mais. Esse processo demorado impede a inovação e pode atrasar o aprendizado e a pesquisa.

A computação em nuvem resolve muitos desses desafios. A nuvem fornece recursos de pay-as-you-go TI sob demanda, para que você possa combinar mais de perto a capacidade atual com as demandas reais sem grandes planejamentos e investimentos iniciais. No entanto, se você já fez um investimento significativo em hardware e recursos on-premises, deve procurar utilizar esses recursos de forma eficiente e aumentá-los conforme necessário com a tecnologia de nuvem em um modelo híbrido.

Uma estratégia de nuvem híbrida bem-sucedida aproveita os investimentos existentes e, ao mesmo tempo, fornece maior agilidade, escalabilidade e confiabilidade do que esses investimentos sozinhos podem oferecer. Os conceitos a seguir ajudarão você a começar a usar.

- Quando você precisa hospedar uma nova workload, você pensa primeiro na nuvem?

  A forma como você usa a infraestrutura de nuvem pública e privada em conjunto define sua estratégia de nuvem híbrida. Uma abordagem que prioriza a nuvem não significa que a nuvem seja a melhor opção para todas as suas workloads. No entanto, ao planejar novas workloads, avalie a nuvem como a primeira opção, especialmente para workloads que exigem novas tecnologias ou excedem a capacidade de armazenamento e computação disponível on-premises. Workloads que têm padrões de uso transitórios e inconsistentes, precisam de resultados rápidos, são facilmente transportáveis ou exigem o hardware mais novo são candidatas ideais para a escalabilidade e elasticidade da nuvem. Além disso, considere se a workload se beneficiaria de quaisquer serviços gerenciados nativos da nuvem que não estejam disponíveis on-premises, mesmo que você tenha capacidade disponível.
- Você entende o TCO do seu ambiente on-premises e faz parceria com seu diretor financeiro ao fazer novos investimentos?

  Recomendamos que você entenda o verdadeiro custo total de propriedade (TCO) de manter seu próprio data center on-premises. Há muitos custos ocultos associados à propriedade e operação da infraestrutura on-premises, incluindo não apenas hardware, software e suporte, mas também instalações, serviços públicos, seguros e horas de trabalho da equipe. Esses custos podem afetar negativamente a produtividade da equipe, a resiliência operacional e a agilidade dos negócios. Avalie suas estruturas de licenciamento atuais e também seus períodos de renovação e manutenção. A parceria com seu diretor financeiro (CFO) pode ajudar você a identificar todos os custos ocultos quando for planejar fazer novos investimentos. Algumas licenças podem oferecer opções de traga a sua própria licença (BYOL) na nuvem, ou podem ser mais ou menos propícias aos serviços em nuvem. Entender o verdadeiro TCO da sua infraestrutura atual ajuda você a priorizar a adoção da nuvem para workloads que têm o maior impacto no TCO total da sua organização. Sua equipe de AWS contas tem ferramentas prontamente disponíveis para ajudar você a entender melhor seu TCO local.
- De qual infraestrutura você precisará para oferecer suporte às implantações híbridas?

  Para adotar modelos híbridos com êxito, você precisará de ferramentas básicas de rede, segurança e infraestrutura. Certifique-se de que você possa manter a conectividade de rede adequada com seu provedor de nuvem. Isso pode ocorrer por meio de uma combinação de

conectividade à Internet existente, redes privadas virtuais (VPNs), conexões dedicadas Direct Connect, como provedores de conectividade terceirizados, ou Internet2 e redes regionais de pesquisa e educação. Verifique se você tem gerenciamento unificado de identidade e acesso em seus ambientes on-premises e de nuvem. Estabeleça ferramentas e processos para impor barreiras de proteção consistentes de segurança, custo e uso.

- Sua equipe de TI está pronta para operar implantações híbridas?

  Os serviços em nuvem podem exigir competências específicas que sua equipe talvez não tenha. Para limitar o treinamento e a capacitação necessários para requalificar sua equipe de TI para uma adoção eficaz da nuvem, verifique se o provedor de nuvem oferece serviços que reutilizam e se baseiam nas competências existentes on-premises e na nuvem. Por exemplo, se você usa e está familiarizado com o Kubernetes, considere usar o Amazon Elastic Kubernetes Service (Amazon EKS) ou o Amazon EKS Anywhere. Se você usa e está familiarizado NetApp, considere usar a Amazon FSx para NetApp ONTAP. Da mesma forma, considere também se alguma solução de parceiro existente que você usa tem integrações nativas ou suporte para ambientes de nuvem.

- Você pode transferir o armazenamento de longo prazo ou a computação de baixo uso do local para a nuvem?

  O armazenamento em nuvem oferece várias opções econômicas para armazenamento de dados de longo prazo. Por exemplo, o Amazon Simple Storage Service (Amazon S3) oferece várias camadas de armazenamento que são otimizadas para diferentes casos de uso. Se sua instituição precisar manter determinados dados por um longo período de tempo, considere soluções de armazenamento frio, como o Amazon Glacier. Transferir esses dados para o armazenamento em nuvem pode liberar um valioso armazenamento on-premises de alta performance. Serviços como o AWS Storage Gateway facilitam o acesso de aplicações on-premises às camadas de armazenamento em nuvem por meio de protocolos padrão, como SMB, NFS e iSCSI. Da mesma forma, considere descarregar qualquer tarefa de computação que tenha uso infrequente ou baixo. Se você tiver servidores on-premises dedicados a essas tarefas, poderá usar serviços de computação em nuvem escaláveis, em que os recursos são provisionados sob demanda e você paga somente pelo que usa. Essas opções de armazenamento de baixo custo e longo prazo e computação de baixo uso também tornam a nuvem ideal para backup e recuperação de desastres. Você pode usar armazenamento e computação seguros, duráveis e escaláveis na nuvem para proteger seus dados e se recuperar rapidamente em caso de desastre, sem precisar manter a infraestrutura de armazenamento e computação necessária por conta própria.

- Você tem capacidade suficiente on-premises para experimentar e inovar?

A falta de elasticidade e agilidade em ambientes on-premises de tamanho fixo pode limitar os serviços e a tecnologia disponíveis para seus usuários. Se você tiver ciclos de atualização rígidos, as novas workloads talvez precisem esperar até o próximo ciclo para serem implementadas. Esse modelo operacional pode limitar a experimentação e retardar a inovação. Quando você tem uma workload nova ou inédita que precisa ser testada, considere usar serviços de nuvem escaláveis e elásticos. Os recursos de nuvem podem ser provisionados e desprovisionados sob demanda, e você paga somente pelo que usa, para que possa experimentar e antecipar-se à falha, minimizando o risco organizacional.

- Você tem requisitos exclusivos de conformidade ou performance que obrigam você a manter os dados on-premises?

  Workloads com requisitos rígidos de latência ou residência de dados podem exigir que você mantenha os dados on-premises ou o mais próximo possível dos usuários. Para esses casos de uso, você pode priorizar o uso de recursos on-premises existentes. No entanto, considere se seu provedor de nuvem oferece serviços ou mecanismos de borda para usar a tecnologia baseada em nuvem on-premises. Os serviços de borda oferecem processamento, análise e armazenamento de dados mais perto de seus próprios endpoints e permitem que você implante ferramentas fora dos data centers padrão dos provedores de nuvem. Por exemplo, a AWS oferece serviços como Zonas locais da AWS e o AWS Wavelength para implantar aplicações em locais específicos mais próximos dos usuários finais. Você também pode trazer serviços e funcionalidades de nuvem para seu data center existente com serviços como o AWS Outposts, AWS Storage Gateway, Amazon ECS Anywhere e Amazon EKS Anywhere.

Reservar a multinuvem somente para workloads que não podem atender aos requisitos técnicos ou comerciais por meio de um único provedor de nuvem

Multinuvem refere-se ao uso de serviços em nuvem de vários (dois ou mais) provedores de serviços em nuvem. Ter uma estratégia multinuvem pode oferecer certas vantagens, como a opção de descobrir os recursos diferenciados de vários provedores de nuvem ou a capacidade de atender aos requisitos de soberania de dados que um único provedor de nuvem talvez não consiga acomodar. No entanto, para cada provedor que você usa, certifique-se de ter as pessoas, as habilidades, o treinamento e as competências adequadas para usar esse provedor de forma eficaz. Além disso, se quiser usar uma estratégia multinuvem para uma workload específica, você precisará de

recursos adicionais para integrar e interoperar os serviços necessários de cada provedor de nuvem. Recomendamos que você considere a multinuvem somente quando as vantagens superarem o aumento do investimento. Para determinar se você deve escolher uma estratégia de multinuvem, considere as perguntas-chave a seguir.

- Você tem os recursos e as capacidades para lidar com os serviços oferecidos por diferentes provedores de nuvem?

  Quando vários provedores de nuvem oferecem vários produtos e serviços, sua equipe precisa ter habilidades essenciais para lidar com os recursos de cada provedor. Usar os serviços de apenas um provedor de nuvem pode exigir requalificação e treinamento da sua equipe, dependendo dos serviços e recursos que você está usando. Se você estiver considerando uma estratégia multinuvem, avalie seus recursos existentes para determinar de quais competências adicionais você precisaria para usar os serviços de vários provedores de nuvem de forma eficaz. Talvez você precise aumentar sua equipe ou investir mais tempo e dinheiro em requalificação e treinamento, além do que seria necessário para um único provedor de nuvem. Se você já tem equipes ou usuários individuais que estão usando diferentes provedores de nuvem, considere os benefícios organizacionais de consolidá-los em um provedor de nuvem primário em uma case-by-case base.
- Que sobrecarga adicional uma arquitetura multinuvem específica introduziria?

  Um fator comum para a multinuvem é o desejo de usar um serviço gerenciado específico de um provedor que tenha recursos que possam ser diferenciados dos serviços de outro provedor de nuvem. Por exemplo, talvez você precise usar um provedor de nuvem para as necessidades de infraestrutura e o serviço gerenciado de outro provedor para serviços de domínio e diretório. No entanto, mesmo que esse único serviço gerenciado reduza a carga administrativa e simplifique o gerenciamento desse componente de arquitetura, ele pode introduzir uma sobrecarga adicional para outras workloads, como refatoração de código, necessidades de conectividade privada ou trabalho de integração manual. Identifique esse custo adicional logo de início e certifique-se de que ele não anule ou ofusque as vantagens que sua equipe pode obter com o serviço diferenciado.
- Como você centralizará o monitoramento e o gerenciamento entre os provedores de nuvem?

  Ao começar a implantar aplicações e funcionalidades usando recursos de diferentes provedores de nuvem, considere como você identificará, monitorará e gerenciará esses recursos. Cada provedor terá suas próprias ferramentas, que você poderá estender para outros ambientes. Por exemplo, você pode usar CloudWatch a Amazon para monitorar as principais métricas e registros, criar alarmes e visualizar seus aplicativos e infraestrutura em ambientes de nuvem única, híbrida e multicloud. Você também pode usar o AWS Systems Manager para melhorar a visibilidade e o

controle dos recursos, diagnosticar e remediar problemas operacionais rapidamente e automatizar processos como atualização e aplicação de patches em máquinas virtuais em vários ambientes. Se você tem requisitos a que as ferramentas de um provedor não atendem, você pode analisar soluções de parceiros, mas elas podem adicionar custos adicionais ou esforço de integração.

- Como você pode gerenciar a infraestrutura como código com automação ao usar diferentes provedores de nuvem?

  Quando você executa recursos na nuvem, o provisionamento e o gerenciamento automatizados de recursos ajudam a gerenciar vários ambientes com eficiência. As ferramentas de automação nativas APIs e as ferramentas de automação variam entre os provedores de nuvem. Se possível, considere usar um conjunto comum de ferramentas de orquestração e implantação que possa acomodar diferentes recursos de provedores de nuvem. Isso proporciona maior flexibilidade e simplifica as operações em várias nuvens. No entanto, pode ser mais simples usar a automação nativa de cada provedor separadamente e estabelecer processos organizacionais para garantir o uso adequado.
- Você tem requisitos regulatórios e de conformidade que cada provedor de nuvem deve satisfazer?

  Você pode ter considerações regulatórias que determinem como os dados devem ser armazenados e tratados. Concentre-se na padronização de políticas (como tráfego de rede, armazenamento e segurança) que podem ser aplicadas automaticamente a cada ambiente de nuvem em todos os provedores de nuvem. Considere como suas aplicações se comunicarão com seus dados e os hospedarão no mesmo provedor. Se suas aplicações e seus dados estiverem fragmentados entre os provedores, será difícil garantir que você esteja atendendo aos requisitos regulatórios e de conformidade. Geralmente, é melhor ter aplicações o mais próximo possível dos dados para minimizar a latência da rede, maximizar o throughput de dados e limitar a saída de dados, ao mesmo tempo em que simplifica os controles de segurança e acesso.
- Você consegue minimizar o TCO e maximizar os descontos nos preços ao implantar aplicações em provedores de nuvem?

  É importante analisar o custo total de propriedade (TCO) ao considerar multinuvem. Executar suas aplicações em vários provedores de nuvem pode aumentar os custos operacionais e a sobrecarga administrativa para manter e gerenciar recursos em cada ambiente. Além disso, distribuir o uso entre vários provedores dificulta aproveitar os descontos de preços por volume ou os contratos corporativos de um provedor específico. Leve esses fatores em consideração ao determinar se as vantagens da multinuvem justificam o aumento do TCO.

Exemplo de casos de uso

Para entender melhor a aplicação desses princípios em diferentes cenários, vamos discutir alguns exemplos de casos de uso. Esses casos de uso são baseados em como as instituições educacionais do mundo real estão adotando serviços em nuvem.

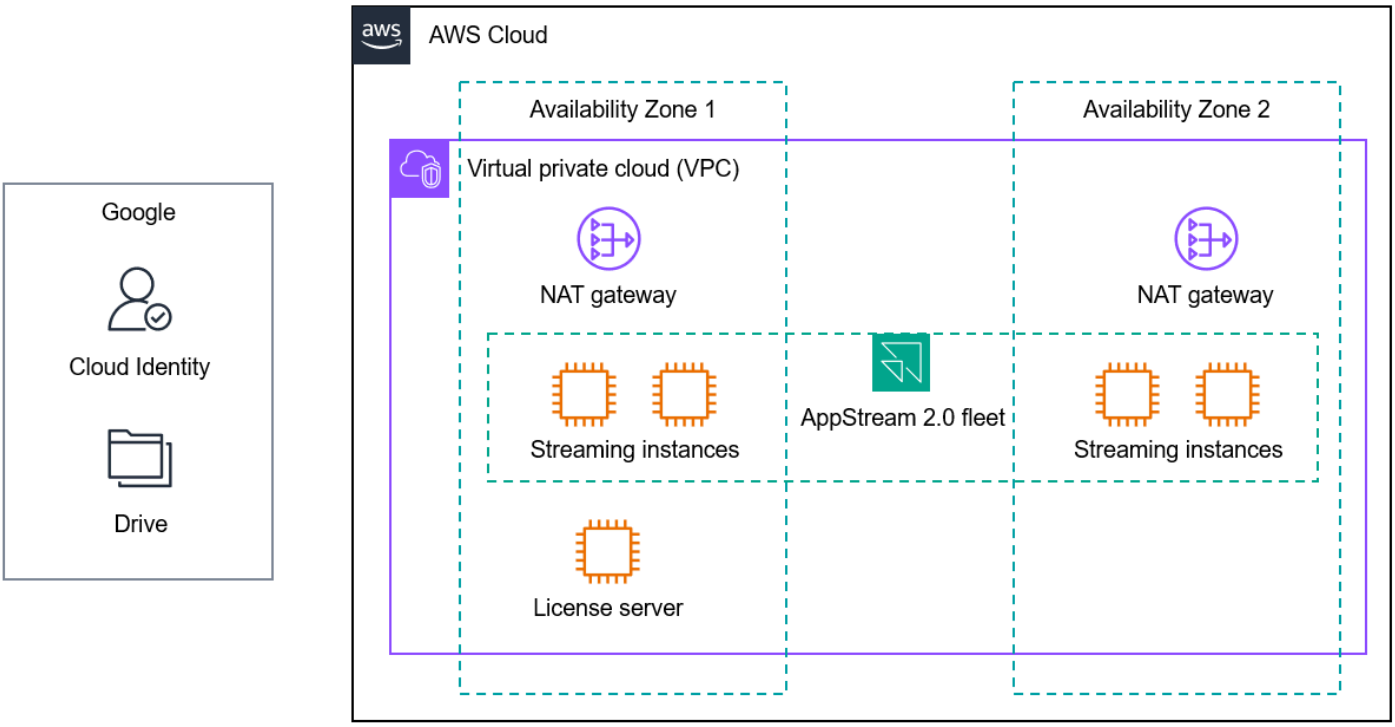
- Laboratórios de computação virtual
- Predição do sucesso estudantil
- Federação de identidades e autenticação única
- Expansão na nuvem para computação de pesquisa

Laboratórios de computação virtual

Apesar da popularidade das ferramentas de aprendizado baseadas na web e da abundância de dispositivos de usuário, como laptops, Chromebooks e tablets, a maioria das instituições educacionais mantém laboratórios físicos de computação para aplicações legadas ou que consomem muitos recursos. Esses laboratórios de computação geralmente são necessários para ciências, tecnologia, engenharia e matemática (STEM), educação profissional e técnica (CTE), mídia e arte, engenharia e currículos similares. As escolas podem ampliar ou substituir os laboratórios físicos de computação por desktops virtuais baseados em nuvem ou serviços de streaming de aplicativos para garantir que todos os alunos tenham acesso às aplicações de que precisam a qualquer momento, em qualquer lugar e em qualquer dispositivo. Isso melhora a equidade digital, permite o aprendizado remoto, garante uma experiência de usuário consistente e protege o acesso remoto, reduzindo os custos.

No ensino fundamental e médio (K12), muitas escolas dos EUA usam o Amazon WorkSpaces Applications, um serviço totalmente gerenciado de streaming de aplicativos e desktops, para oferecer laboratórios virtuais de computação para fornecer acesso à Adobe Creative Cloud, ao software da Autodesk, aos currículos STEM e CTE, como o Project Lead the Way (PLTW) e muito mais. Muitas organizações de ensino fundamental e médio já gerenciam a autenticação única e o armazenamento de arquivos para estudantes por meio do Google Workspace e do Google Drive, que são aplicações SaaS. Essas instituições podem configurar o login único entre o Google Workspace e os WorkSpaces aplicativos por meio da federação SAML 2.0. Eles também podem configurar a integração nativa entre os WorkSpaces aplicativos e o Google Drive para que os alunos possam usar

o armazenamento existente. O diagrama a seguir ilustra a implantação de WorkSpaces aplicativos para esse caso de uso.



Essa arquitetura segue estas recomendações:

- Selecione um provedor de nuvem primário e estratégico.Essa arquitetura usa serviços de nuvem de um provedor de nuvem primário. Embora ela inclua a integração com aplicações SaaS que não estão hospedadas no mesmo provedor, essas integrações são feitas por meio de configurações simples. A experiência e as competências em nuvem são necessárias somente para implantar e gerenciar serviços do provedor de nuvem primário.
- Diferencie entre aplicações SaaS e serviços básicos em nuvem.O Google Workspace e o Google Drive não estão hospedados no mesmo provedor de nuvem do AppStream 2.0, mas isso é aceitável porque essa implantação fornece as integrações necessárias. A autenticação única permite o gerenciamento centralizado de identidades e é configurada com segurança por meio do SAML 2.0. Habilitar o armazenamento em nuvem persistente para estudantes exige mudanças simples de configuração no Google Drive e nos WorkSpaces aplicativos.
- Estabeleça requisitos de segurança e governança para cada provedor de serviços de nuvem.Os serviços e integrações usados nessa arquitetura ajudam a atender aos requisitos de segurança e governança de uma instituição. O tráfego de streaming é criptografado. A federação por meio do Google Workspace permite o gerenciamento centralizado de identidades. Os serviços de

rede como a Amazon Virtual Private Cloud (Amazon VPC) são compatíveis com a configuração de sub-redes, roteamento e firewalls. Você pode filtrar o conteúdo usando a configuração de DNS, agentes, dispositivos virtuais ou serviços gerenciados, como o Firewall de DNS do Amazon Route 53 Resolver . Você pode usar serviços como AWS Control Towerpara ajudar a garantir que a conta da AWS que hospeda os WorkSpaces aplicativos cumpra as barreiras e controles organizacionais padrão.

- Adote soluções gerenciadas nativas da nuvem sempre que possível e prático. WorkSpaces O Applications é um serviço gerenciado para streaming de desktops e aplicativos. Você pode fazer streaming de áreas de trabalho e aplicações sem se preocupar com provisionamento, escalabilidade ou manutenção de servidores. Você instala suas aplicações, conecta as soluções apropriadas de identidade, rede e armazenamento e, em seguida, gerencia e transmite de forma centralizada essas aplicações para seus usuários. Isso elimina grande parte do trabalho pesado indiferenciado que seria necessário para gerenciar sua própria solução de streaming de área de trabalho virtual.

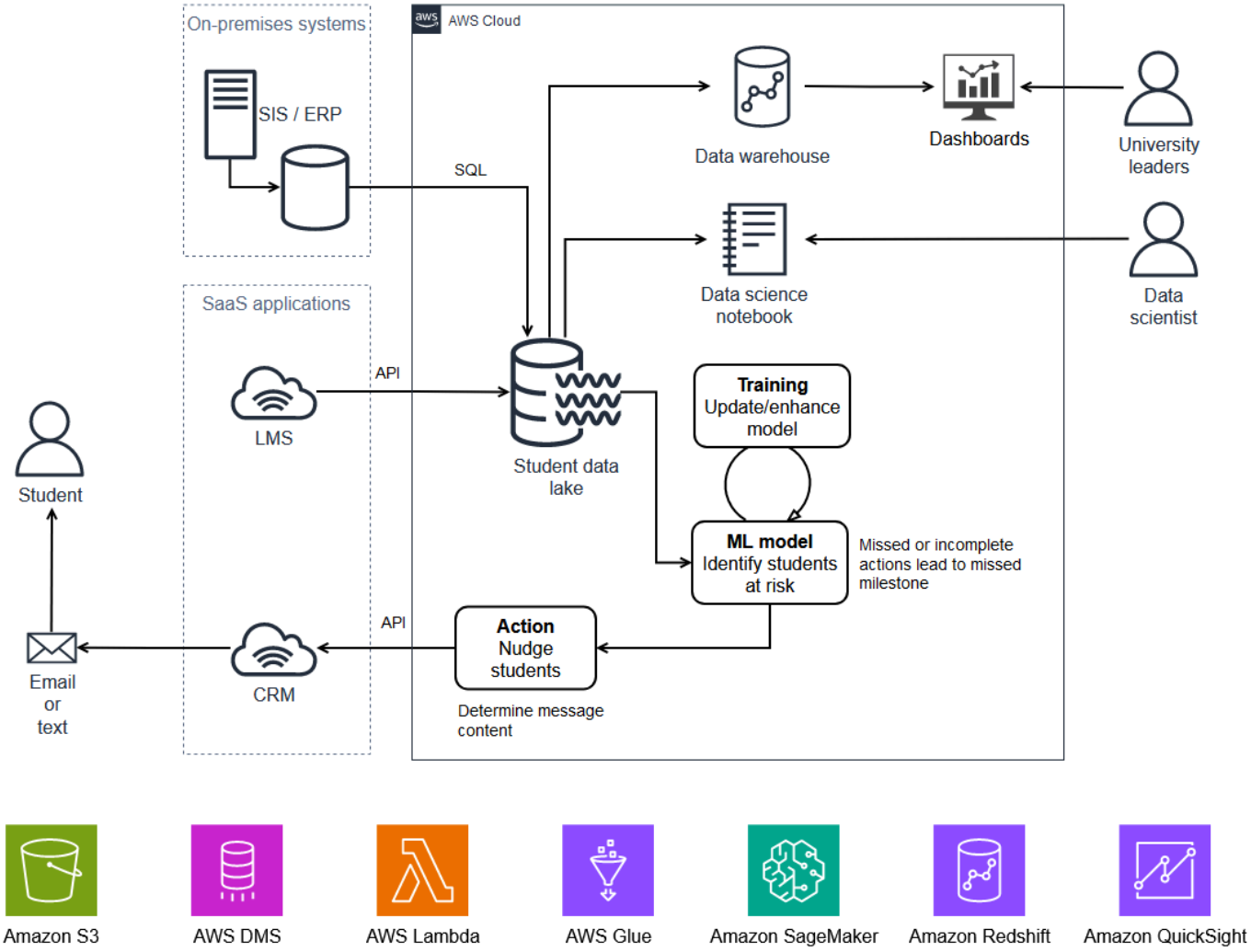
Predição do sucesso estudantil

Uma universidade do Centro-Oeste dos EUA descobriu que algumas atividades importantes para os novos alunos do primeiro ano eram altamente preditivas de sucesso, tanto no primeiro semestre de aulas do aluno quanto na obtenção do diploma. A universidade desejava implementar um sistema que monitorasse a conclusão dessas atividades e que, quando os prazos importantes se aproximassem ou fossem ultrapassados, incentivasse os estudantes a finalizar essas etapas.

Os dados do sistema de gerenciamento de aprendizado (LMS) SaaS foram uma entrada fundamental para essa solução, mas seus dados provaram ser difíceis de acessar e processar com as ferramentas de armazenamento de dados da equipe de TI da universidade. Além disso, as mensagens para os alunos precisavam ser enviadas por meio do sistema de gerenciamento de relacionamento com o cliente (CRM) baseado em nuvem da escola. Para criar uma solução funcional e avaliar a eficácia dos prompts para os alunos, a universidade teve que iniciar mensagens por meio do CRM e coletar dados dele.

A universidade desenvolveu e implantou uma solução em um único ambiente de nuvem. A solução é uma mistura de serviços gerenciados nativos da nuvem, servidores em nuvem provisionados e integrações com sistemas on-premises e aplicações SaaS baseadas na nuvem. Como mostra o diagrama a seguir, a solução ingere dados do sistema de informações estudantis (SIS), do LMS e do CRM em um data lake. Ele usa esses dados para identificar estudantes que correm o risco de perder

atividades importantes, inicia mensagens para eles por meio do CRM e fornece um painel para a liderança da universidade.



Essa arquitetura segue estas recomendações:

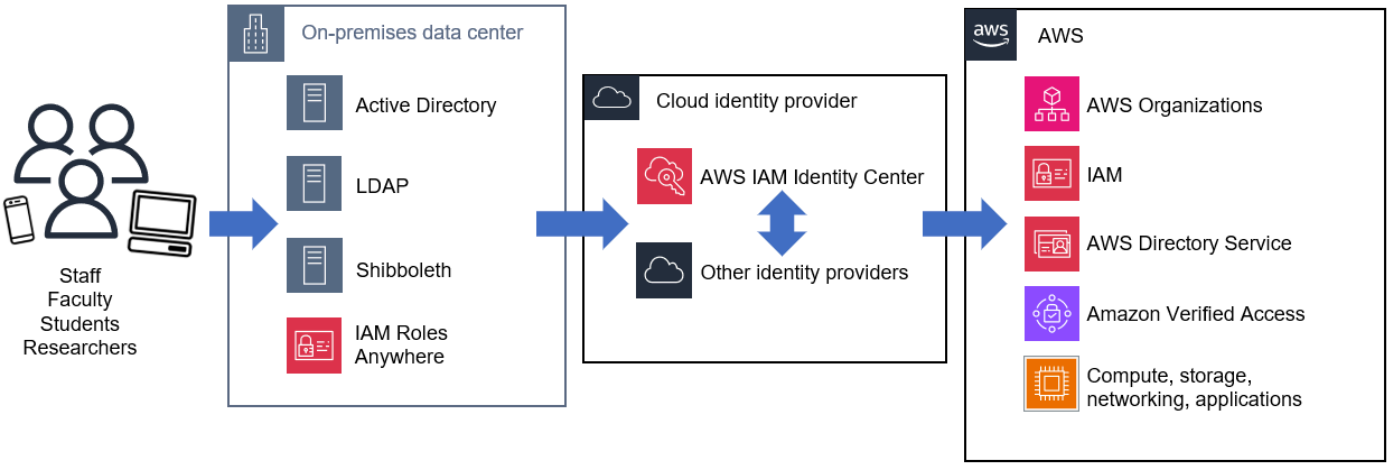
- Selecione um provedor de nuvem primário e estratégico.O provedor estratégico de nuvem da universidade hospeda toda a solução implantada. Isso permite que a equipe de TI e de negócios se concentre no desenvolvimento de habilidades em um único conjunto integrado de recursos de nuvem.
- Diferencie entre aplicações SaaS e serviços básicos em nuvem.A universidade diferencia entre aplicações SaaS e serviços básicos de analytics em nuvem e usa integrações com as aplicações SaaS para coletar dados e iniciar as comunicações apropriadas.

- Estabeleça requisitos de segurança e governança para cada provedor de serviços de nuvem.A universidade garante que todos os componentes da arquitetura estejam seguros aplicando controles e barreiras de proteção, incluindo criptografia em trânsito e em repouso, para lidar com os dados dos estudantes de forma adequada.
- Adote soluções gerenciadas nativas da nuvem sempre que for possível e prático. Os serviços gerenciados nativos da nuvem são usados para ingestão, armazenamento, banco de dados e funcionalidade de extração, transformação e carregamento (ETL) de dados, o que reduz o tempo de desenvolvimento do fluxo de trabalho de processamento de dados. end-to-end

Federação de identidades e autenticação única

Garantir o gerenciamento consistente de identidades em todos os sistemas centrais é fundamental para adotar com êxito e segurança qualquer tecnologia. As instituições educacionais estão adotando cada vez mais soluções de identidade e login único baseadas em nuvem, como Centro de Identidade do AWS IAMMicrosoft Entra ID (antigo Azure Active Directory), Okta,,, Ping Identity, e CyberArk para simplificar o gerenciamento de identidades, reduzir a carga operacional e aplicar centralmente as melhores práticas, como autenticação multifator e acesso com privilégios mínimos. JumpCloud OneLogin

Muitas dessas instituições ainda mantêm serviços de gerenciamento de identidades e diretórios, como o Active Directory e o Shibboleth, para seus ambientes on-premises. Eles podem ser integrados a soluções baseadas em nuvem para permitir o gerenciamento centralizado de identidades e a autenticação única para os estudantes, corpo docente e funcionários. Os provedores de soluções em nuvem devem ter plataformas robustas de gerenciamento de easy-to-integrate identidade que permitam federar identidades por meio de provedores de identidade em nuvem para seus aplicativos existentes, suas soluções SaaS e serviços em nuvem. O diagrama a seguir mostra um exemplo de arquitetura.



Essa arquitetura segue estas recomendações:

- Selecione um provedor de nuvem primário e estratégico.Essa arquitetura é usada AWS como principal provedor de nuvem. Ao se integrar a um provedor de identidades na nuvem e aos serviços existentes de gerenciamento de identidades e diretório on-premises, essa arquitetura oferece suporte ao provisionamento e ao gerenciamento automatizados do acesso aos serviços do provedor de nuvem primário e a outras aplicações e soluções SaaS. Isso garante que os requisitos de segurança e governança sejam atendidos de forma consistente e sejam fáceis de gerenciar à medida que mais aplicações e serviços são adicionados ao portfólio de tecnologia da instituição.
- Diferencie entre aplicações SaaS e serviços básicos em nuvem.Essa arquitetura integra vários tipos de sistemas de identidade baseados em nuvem, SaaS e locais para fornecer acesso a serviços e outros aplicativos. Nuvem AWS Muitos provedores de identidade baseados em nuvem e soluções de autenticação única também são aplicações SaaS e podem usar integrações nativas e protocolos padrão, como SAML, para trabalhar em vários ambientes.
- Estabeleça requisitos de segurança e governança para cada provedor de serviços de nuvem.Essa arquitetura segue as orientações sobre gerenciamento de identidade e acesso emitidas por vários frameworks de segurança, incluindo o Cybersecurity Framework (CSF) do Instituto Nacional de Padrões e Tecnologia (NIST), NIST 800-171 e NIST 800-53. As integrações com o AWS Organizations, o AWS Identity and Access Management (IAM) e outros serviços de segurança, identidade e conformidade da AWS ajudam a fornecer controles de acesso seguros e granulares com base nas permissões do grupo.
- Adote serviços gerenciados nativos da nuvem sempre que for possível e prático. Essa arquitetura usa serviços gerenciados baseados em nuvem para gerenciamento de identidades e autenticação

única. Isso diminui o tempo e a energia gastos no gerenciamento da infraestrutura e facilita a manutenção desses sistemas críticos.

- Implemente arquiteturas híbridas quando os investimentos on-premises existentes justificarem o uso contínuo. Essa arquitetura integra investimentos on-premises existentes em infraestrutura para hospedar workloads do Active Directory, do Lightweight Directory Access Control (LDAP) e do Shibboleth, e fornece um caminho para, eventualmente, transferir os principais serviços de identidade para a infraestrutura baseada em nuvem. Além disso, se suas cargas de trabalho locais precisarem de acesso baseado em certificado aos AWS recursos, você poderá usar o Roles Anywhere.AWS Identity and Access Management

Expansão na nuvem para computação de pesquisa

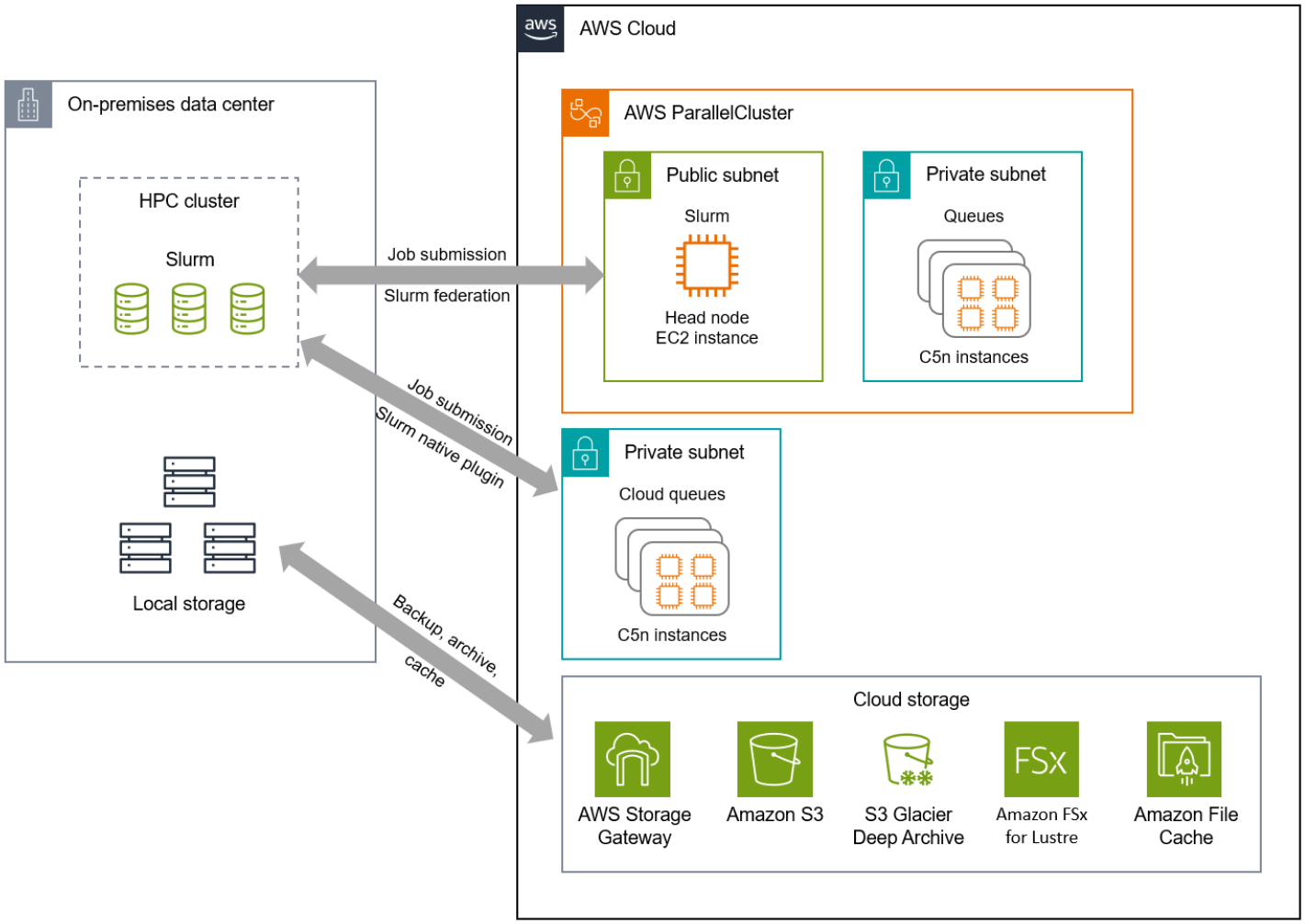
O grupo de computação de pesquisa de uma instituição de pesquisa R1 (Doctoral Universities – Very High Research Activity) nos EUA já executava clusters de computação de alta performance (HPC) on-premises com o agendador Slurm há muitos anos. Com exceção de algumas semanas de manutenção programada, os clusters estavam funcionando com uma taxa de utilização de 80 a 95%, com a maioria das filas cheias.

O número crescente de atividades de pesquisa na instituição introduziu desafios de capacidade e capacitação. Alguns pesquisadores de alto nível estavam sempre realizando simulações de longa duração em determinadas filas, o que aumentava o tempo de espera de outros usuários. O corpo docente recém-contratado precisou executar um grande número de simulações climáticas para criar um novo modelo de inteligência artificial e machine learning (IA/ML) para previsão do tempo, mas exigia mais capacidade do que a disponível. O grupo de pesquisa em computação também estava recebendo mais solicitações para as unidades de processamento gráfico (GPUs) mais recentes para treinar modelos de aprendizado de máquina. Mesmo com o financiamento para novos GPUs, a equipe precisaria esperar meses para obter aprovação para expandir o espaço de rack no data center.

Muitos pesquisadores não estavam dispostos a excluir dados antigos, então a capacidade de armazenamento local também era um desafio. Era necessária uma opção de armazenamento mais escalável e de longo prazo para liberar armazenamento valioso e de alta performance on-premises.

A nuvem aborda esses desafios com soluções híbridas de computação e armazenamento que permitem que você expanda a computação de pesquisa para a nuvem quando a capacidade on-premises não é suficiente. O diagrama de arquitetura a seguir ilustra algumas abordagens de

expansão de computação e armazenamento, usando ferramentas como AWS ParallelCluster e AWS Storage Gateway.



Essa arquitetura segue estas recomendações:

- Selecione um provedor de nuvem primário e estratégico.Essa arquitetura usa um provedor de nuvem primário para evitar ser restringida pela abordagem do mínimo denominador comum. Dessa forma, a instituição pode aproveitar a inovação e os serviços nativos de computação e armazenamento que o provedor de nuvem primário oferece. A equipe de computação de pesquisa pode se concentrar na otimização das workloads no ambiente fornecido pelo provedor de nuvem primário, e não em como trabalhar em diferentes ambientes de nuvem.
- Estabeleça requisitos de segurança e governança para cada provedor de serviços de nuvem.Cada serviço e ferramenta usados nessa arquitetura podem ser configurados para atender aos requisitos de segurança e governança da equipe de computação de pesquisa, incluindo

conectividade privada, criptografia de dados em trânsito e em repouso, registro em log de atividades e muito mais.

- Adote serviços gerenciados nativos da nuvem sempre que for possível e prático. Essa arquitetura fornece a capacidade de usar serviços gerenciados de armazenamento e computação, bem como ferramentas para simplificar o gerenciamento de clusters. Dessa forma, a equipe de computação de pesquisa não precisa se preocupar com o gerenciamento de clusters ou da infraestrutura subjacente por conta própria, o que pode ser complexo e demorado.
- Implemente arquiteturas híbridas quando os investimentos on-premises existentes justificarem o uso contínuo. Essa arquitetura permite que a instituição continue usando seus recursos on-premises e aproveite a nuvem para aumentar a capacidade e expandir a capacidade de computação sob demanda. Com a nuvem, a instituição pode dimensionar corretamente o tipo de computação para maximizar o preço-performance e acessar a tecnologia mais recente para promover a inovação sem um grande investimento inicial em hardware on-premises adicional.

Próximas etapas

Selecionar o modelo de implantação correto para workloads na nuvem exige uma análise cuidadosa. Use as recomendações descritas neste paper para orientar sua tomada de decisão e evitar armadilhas comuns, como complexidade desnecessária, demandas crescentes de pessoal, governança inconsistente e abordagens de menor denominador comum. Seguindo essas práticas recomendadas, você pode acelerar a adoção da nuvem para atingir e superar suas metas institucionais com mais eficiência.

Lembre-se de selecionar um provedor de nuvem principal e estratégico e estabelecer um Centro de Excelência em Nuvem (CCoE) para ajudar a impulsionar a maturidade organizacional e garantir seu sucesso a longo prazo. Diferencie entre aplicações SaaS e serviços básicos em nuvem e identifique os principais requisitos de segurança e governança para cada um. Sempre que possível, adote serviços gerenciados nativos da nuvem e implemente arquiteturas híbridas quando seus investimentos existentes em data center estimularem o uso contínuo. Por fim, reserve a multinuvem somente para as workloads que realmente precisam dela.

AWS está bem posicionado para ajudá-lo a gerenciar ambientes de nuvem única, híbrida e multicloud. Sua instituição pode usar soluções AWS de gerenciamento e observabilidade AWS Systems Manager, como, AWS Config, e CloudWatch a Amazon para simplificar e centralizar o gerenciamento e o monitoramento de sua infraestrutura e aplicativos, independentemente do seu ambiente. Com serviços de dados e analytics, como o Amazon Athena, AWS Glue e AWS DataSync, você pode obter insights de todos os seus dados, onde quer que estejam armazenados. Soluções híbridas AWS Outposts, como, AWS Wavelength, e AWS Snow Familypermitem que você leve AWS infraestrutura e serviços para onde quer que sejam necessários. Ferramentas como o Amazon EKS Distro ajudam você a criar clusters Kubernetes autogerenciados localmente ou em outras nuvens. AWS

Ao definir sua estratégia de nuvem, considere estas próximas etapas:

1. Analise o AWS Cloud Adoption Framework (AWS CAF) para identificar e priorizar oportunidades de transformação, avaliar e melhorar sua prontidão para a nuvem e desenvolver iterativamente seu roteiro de transformação.
2. Identifique um sistema de implementação em nuvem para começar como uma prova de conceito. Isso ajudará você a definir a base ou o framework da nuvem para validar quaisquer suposições, e também possibilitará futuras implementações na nuvem.

3. Envolva sua equipe de AWS contas para discutir suas metas de implementação de nuvem. A equipe de AWS contas pode ajudar a fornecer esclarecimentos, sugerir abordagens, identificar dependências e também trabalhar com suas equipes para mapear sua jornada do conceito inicial à implementação.

Colaboradores

Os colaboradores deste guia incluem:

- Kevin Arand, gerente sênior, arquitetura de soluções, educação, AWS
- Kevin McCandless, arquiteto sênior de soluções, ensino fundamental e médio, AWS
- Craig Jordânia, arquiteto principal de soluções, educação, AWS
- Jesse Roberts, arquiteto principal de soluções, SLG e ensino fundamental e médio e, AWS
- Jianjun Xu, arquiteto principal de soluções, educação, AWS
- Josh Badal, arquiteto sênior de soluções, educação, AWS
- Raj Chary, arquiteto sênior de soluções, educação, AWS

Outras fontes de leitura

Para obter informações adicionais, consulte:

- AWS Centro de Arquitetura da
- Transformação da nuvem no setor público
- AWS Cloud Adoption Framework (AWS CAF)
- Soluções da AWS para nuvem híbrida e multinuvem

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	—	15 de setembro de 2023

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

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

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

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

A

ABAC

Consulte controle de acesso baseado em atributo.

serviços abstraídos

Veja serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

AGGREGATE FUNCTION

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

AI

Veja inteligência artificial.

AIOps

Veja operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicações

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade (ACID)

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

controle de acesso por atributo (ABAC)

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

fonte de dados autorizada

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

Zona de disponibilidade

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

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

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

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

B

bot malicioso

Um bot destinado a causar disrupção ou danos a indivíduos ou organizações.

BCP

Veja planejamento de continuidade de negócios

gráfico de comportamento

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

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também endianness.

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

Acesso de emergência

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

planejamento de continuidade de negócios (BCP)

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

C

CAF

Veja AWS Cloud Adoption Framework.

implantação canário

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

CCoE

Veja Centro de Excelência da Nuvem.

CDC

Veja captura de dados de alteração.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja integração e entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendas 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 corporativa.

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

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

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

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

CMDB

Veja banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

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

desvio de dados

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

dados em trânsito

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

data mesh

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Veja linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

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

implantação

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

ambiente de desenvolvimento

Veja ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Veja linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja recuperação de desastres.

Detecção da oscilação

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

DVSM

Veja mapeamento do fluxo de valor de desenvolvimento.

E

EDA

Veja análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

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

intercâmbio eletrônico de dados (EDI)

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

criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja endpoint de serviço.

serviço de endpoint

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

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

planejamento de recursos empresariais (ERP)

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

criptografia envelopada

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

ambiente

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

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

epic

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

ERP

Veja planejamento de recursos empresariais.

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

Antecipar-se à falha

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

delimitação de isolamento contra falhas

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

ramificação de recursos

Veja ramificação.

recursos

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

importância do recurso

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

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

transformação de recursos

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

prompt few shot

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

FGAC

Veja controle de acesso refinado.

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

FM

Veja modelo de base.

modelo de base (FM)

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

G

IA generativa

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

bloqueio geográfico

Veja restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

golden image

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

estratégia greenfield

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

barreira de proteção

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

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

H

HA

Veja alta disponibilidade.

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

dados de hold-out

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

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

eu

IaC

Veja infraestrutura como código.

Política baseada em identidade

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

aplicação ociosa

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

IIoT

Veja Internet das Coisas Industrial.

infraestrutura imutável

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

VPC de entrada (admissão)

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

migração incremental

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

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

VPC de inspeção

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

Internet das coisas (IoT)

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

interpretabilidade

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

IoT

Veja Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Veja biblioteca de informações de TI.

ITSM

Veja gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

grande modelo de linguagem (LLM)

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em rótulo.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também endianness.

LLM

Veja grande modelo de linguagem.

ambientes inferiores

Veja ambiente.

M

machine learning (ML)

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

ramificação principal

Veja ramificação.

Malware

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

Serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Veja Programa de Aceleração da Migração.

mecanismo

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

conta de membro

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

MES

Veja sistema de execução de manufatura.

Transporte de Telemetria de Enfileiramento de Mensagens (MQTT)

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

microsserviço

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

arquitetura de microsserviços

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

de uma interface bem definida usando leveza. APIs Cada 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: rehospede a migração para o Amazon EC2 AWS com o Application Migration Service.

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja machine learning.

modernização

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

avaliação de preparação para modernização

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

aplicações monolíticas (monólitos)

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

MPA

Veja Avaliação do Portfólio para Migração.

MQTT

Veja Transporte de Telemetria de Enfileiramento de Mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja controle de acesso de origem.

OAI

Veja identidade de acesso de origem.

OCM

Veja gerenciamento de alterações organizacionais.

migração offline

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

OI

Veja integração de operações.

Ola

Veja acordo de nível operacional.

migração online

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

OPC-UA

Veja Open Process Communications - Unified Architecture.

Open Process Communications - Unified Architecture (OPC-UA)

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (TO)

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

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

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

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

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

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

ORR

Veja análise de prontidão operacional.

OT

Veja tecnologia operacional.

VPC de saída (egresso)

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

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja informações de identificação pessoal.

manual

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

PLC

Veja controlador lógico programável.

PLM

Veja gerenciamento do ciclo de vida do produto.

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pushdown de predicados

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

controle preventivo

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

principal (entidade principal)

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

informações, consulte Entidade principal em Termos e conceitos de perfis na documentação do IAM.

Privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja ambiente.

controlador lógico programável (PLC)

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

encadeamento de prompts

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

pseudonimização

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

publish/subscribe (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

Veja responsável, aprovador, consultado, informado (RACI).

RAG

Veja geração aumentada via recuperação.

ransomware

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

Matriz RASCI

Veja responsável, aprovador, consultado, informado (RACI).

RCAC

Veja controle de acesso por linha e coluna.

réplica de leitura

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

Redefinir arquitetura

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

Região

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

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

Retirada

Veja 7 Rs.

Geração Aumentada de Recuperação (RAG)

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

alternância

O processo de atualizar periodicamente um segredo para dificultar o acesso de um invasor às credenciais.

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja objetivo de ponto de recuperação.

RTO

Veja objetivo de tempo de recuperação.

runbook

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

S

SAML 2.0

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

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

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja política de controle de serviço.

secret

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

segurança desde a concepção

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

controle de segurança

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

hardening da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme avaliado por um indicador de nível de serviço.

modelo de responsabilidade compartilhada

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

SIEM

Veja sistema de gerenciamento de eventos e informações de segurança.

ponto único de falha (SPOF)

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

SLA

Veja cacordo de serviço.

SLI

Veja indicador de nível de serviço.

SLO

Veja objetivo de nível de serviço.

split-and-seed modelo

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

SPOF

Veja ponto único de falha.

esquema em estrela

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

padrão strangler fig

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

sub-rede

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

controle supervisório e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

prompt do sistema

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

gerenciamento para você. Para obter mais informações, consulte Usando AWS Organizations com outros AWS serviços na AWS Organizations documentação.

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja ambiente.

V

aspiração

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

controle de versões

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

emparelhamento da VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

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

WORM

Veja gravação única e várias leituras.

WQF

Veja AWS Workload Qualification Framework.

gravação única e várias leituras (WORM)

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

Z

exploração de dia zero

Um ataque, normalmente malware, que tira proveito de uma vulnerabilidade zero-day.

vulnerabilidade de dia zero

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

prompt zero shot

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

aplicação zumbi

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

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