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

AWS Recomendações

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

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

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

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

Table of Contents

Introdução 1
Visão geral do 1
Estratégias de implantação de nuvem 4
Nuvem única 4
Nuvem híbrida 4
Multinuvem 4
Recomendações 5
Selecionar um provedor de nuvem primário e estratégico 5
Estabelecer um CCoE 7
Diferenciar entre aplicações SaaS e serviços básicos em nuvem 10
Estabelecer requisitos de segurança e governança para cada provedor de serviços de nuvem 12
Adotar serviços gerenciados nativos da nuvem sempre que for possível e prático 16
Implementar arquiteturas híbridas quando os investimentos on-premises existentes justificarem o uso contínuo 20
Reservar a multinuvem somente para workloads que não podem atender aos requisitos técnicos ou comerciais por meio de um único provedor de nuvem 23
Exemplo de casos de uso 27
Laboratórios de computação virtual 27
Predição do sucesso estudantil 29
Federação de identidades e autenticação única 31
Expansão na nuvem para computação de pesquisa 33
Próximas etapas 36
Colaboradores 38
Outras fontes de leitura 39
Histórico do documento 40
..... xli

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
- Recomendações
- Exemplos de casos de uso
- Próximas etapas

- Colaboradores
- Outras fontes de leitura
- Histórico de documentos

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
- Estabelecer um CCoE
- 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, provedores de software independente (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.

Estabelecer um CCoE

Considere desenvolver sua função de liderança na nuvem por meio de um escritório de transformação ou de um Centro de Excelência da Nuvem (CCoE). Um CCoE desenvolve e evangeliza uma abordagem para implementar a tecnologia de nuvem em grande escala em toda a organização. Para uma adoção com êxito da nuvem, projete seu CCoE para incluir representantes que possam falar pelas equipes e departamentos envolvidos. Comece em escala reduzida e

desenvolva gradualmente o CCoE para atender às suas necessidades à medida que você avança na jornada de transformação. Seus representantes do provedor de nuvem primário, como seu gerente de conta da AWS e arquiteto de soluções, podem fornecer recursos para orientar você na criação do seu CCoE. Um CCoE acelera sua capacidade de consolidar 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 CCoE.

- Quem você deve incluir em seu CCoE?

  No seu começo, um CCoE pode incluir apenas um pequeno grupo de usuários iniciais e líderes da nuvem. O CCoE pode permanecer pequeno, mas deve evoluir para incluir líderes que representem tanto as áreas de negócios quanto as 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. O CCoE também deve procurar envolver fornecedores e parceiros, conforme necessário, para fornecer experiência no assunto. O CCoE 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 o CCoE interage com suas partes interessadas?

  O CCoE está a serviço de outras equipes e tem como objetivo apenas informar e permitir a adoção com êxito da nuvem. Veja a incorporação de partes do CCoE 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 CCoE deve ter mecanismos definidos para se comunicar com as partes interessadas, coletar feedback e treinar usuários. As métricas de sucesso do CCoE 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 avaliar coisas como o número de equipes que se tornam autossuficientes por meio do trabalho do CCoE, o número de vezes que o CCoE é crucial para as iniciativas, a quantidade de eventos de treinamento realizados ou a abrangência da adoção dos

resultados do CCoE. Um CCoE bem construído e confiável pode ser o ponto de partida para uma transformação organizacional maior baseada na confiança.

- Como você deve estabelecer um CCoE?

  A maioria das organizações inicia a adoção da nuvem com projetos piloto específicos e direcionados. Estabeleça um CCoE 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 de APIs protegidas com mecanismos apropriados de autenticação e autorização. 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, APIs privadas ou interfaces privadas, como o AWS PrivateLink, para 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, proteção distribuída AWS Shieldde 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:

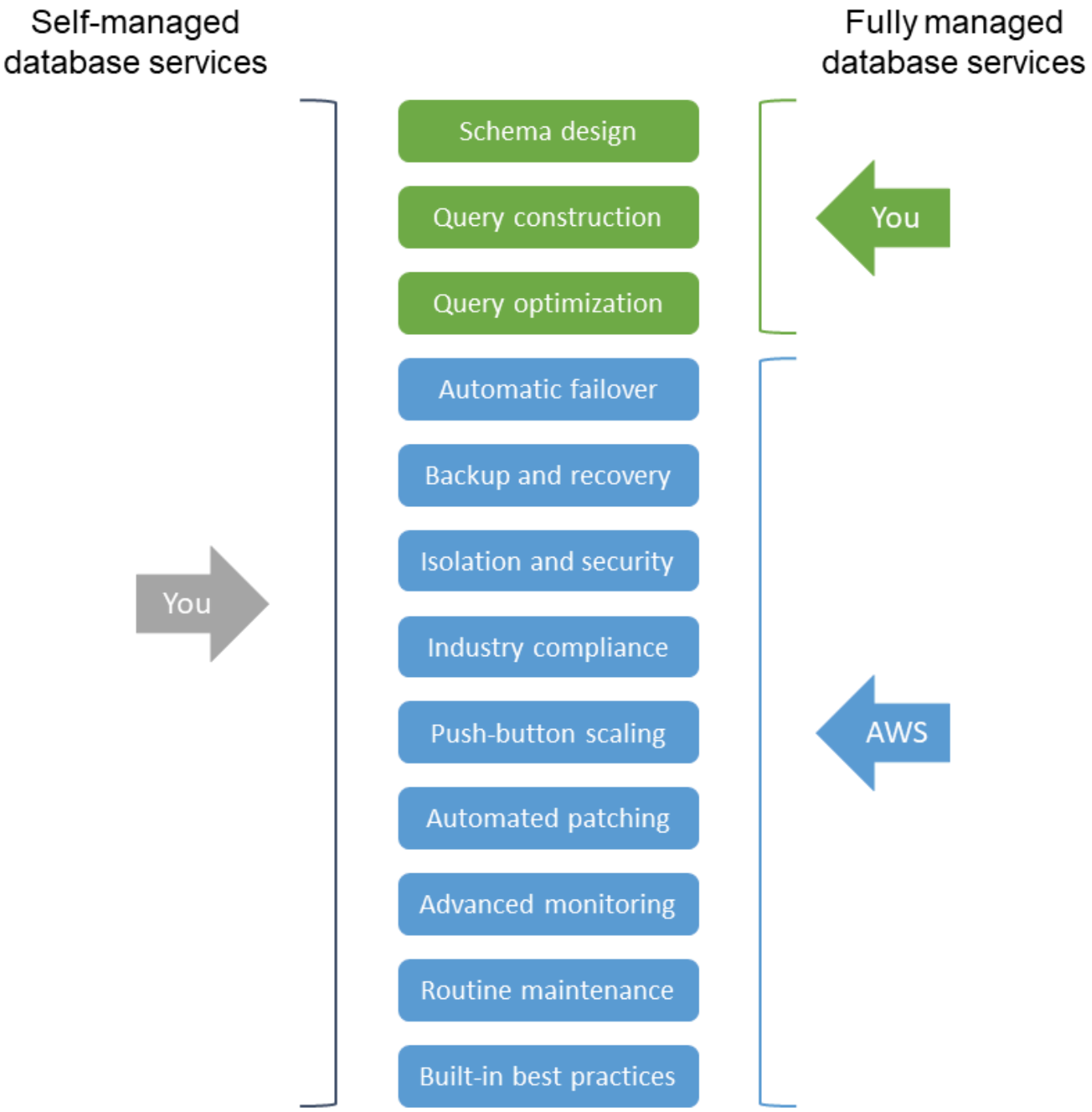
  - Concentre seus esforços em medidas preventivas na forma de controles de segurança que são incorporados automaticamente em ambientes de nuvem.
  - Implemente recursos de detecção que ajudem as equipes de resposta a incidentes cibernéticos a detectar, conter e mitigar violações de segurança em tempo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

Cloud-native, os serviços gerenciados 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 natureza sob demanda e de pagamento conforme o uso 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 APIs específicas do serviço. Mesmo que o serviço use APIs padrão do setor ou de código aberto, talvez seja necessário refatorar ou configurar sua aplicação 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. Tecnologias sem servidor apresentam escalabilidade automática, alta disponibilidade integrada e um modelo de cobrança de pagamento conforme o uso 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 provedores de software independente (ISVs), pode parecer lógico replicar sua implantação on-premises com a infraestrutura de 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 que possível, você deve preferir ISVs que ofereçam recomendações 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 oferecer suporte a padrões e APIs comuns do setor. 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 Lambdasuporta nativamente 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 APIs proprietárias, soluções nativas ou de parceiros podem estar disponíveis para interagir com as 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 TI sob demanda e com pagamento conforme o uso para que você possa alinhar mais de perto a capacidade atual com as demandas reais sem grandes planejamentos e investimentos antecipados. 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 o Amazon FSx for 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 as vantagens organizacionais de consolidá-los em um provedor de nuvem primário, caso a caso.
- 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 APIs e as ferramentas de automação nativas 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.

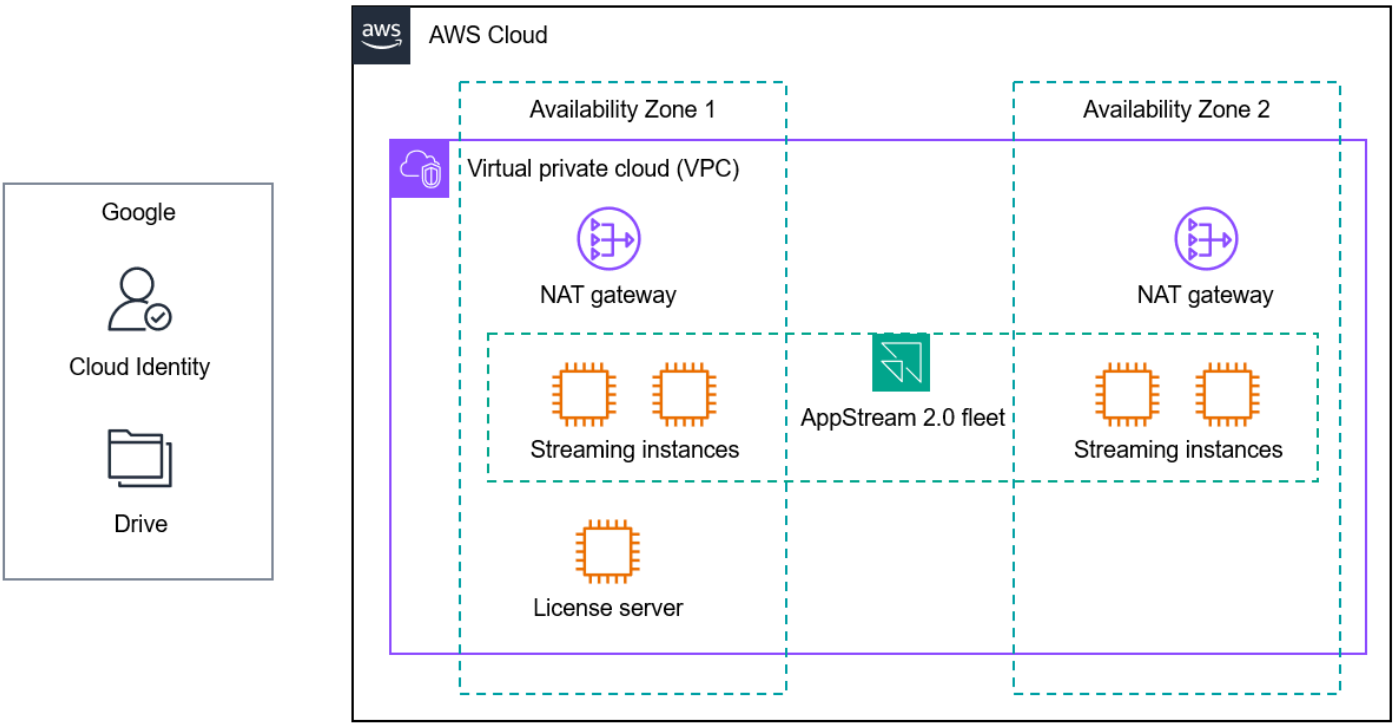
- Laboratórios de computação virtual
- Predição do sucesso estudantil
- Federação de identidades e autenticação única
- Expansão na nuvem para computação de pesquisa

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.

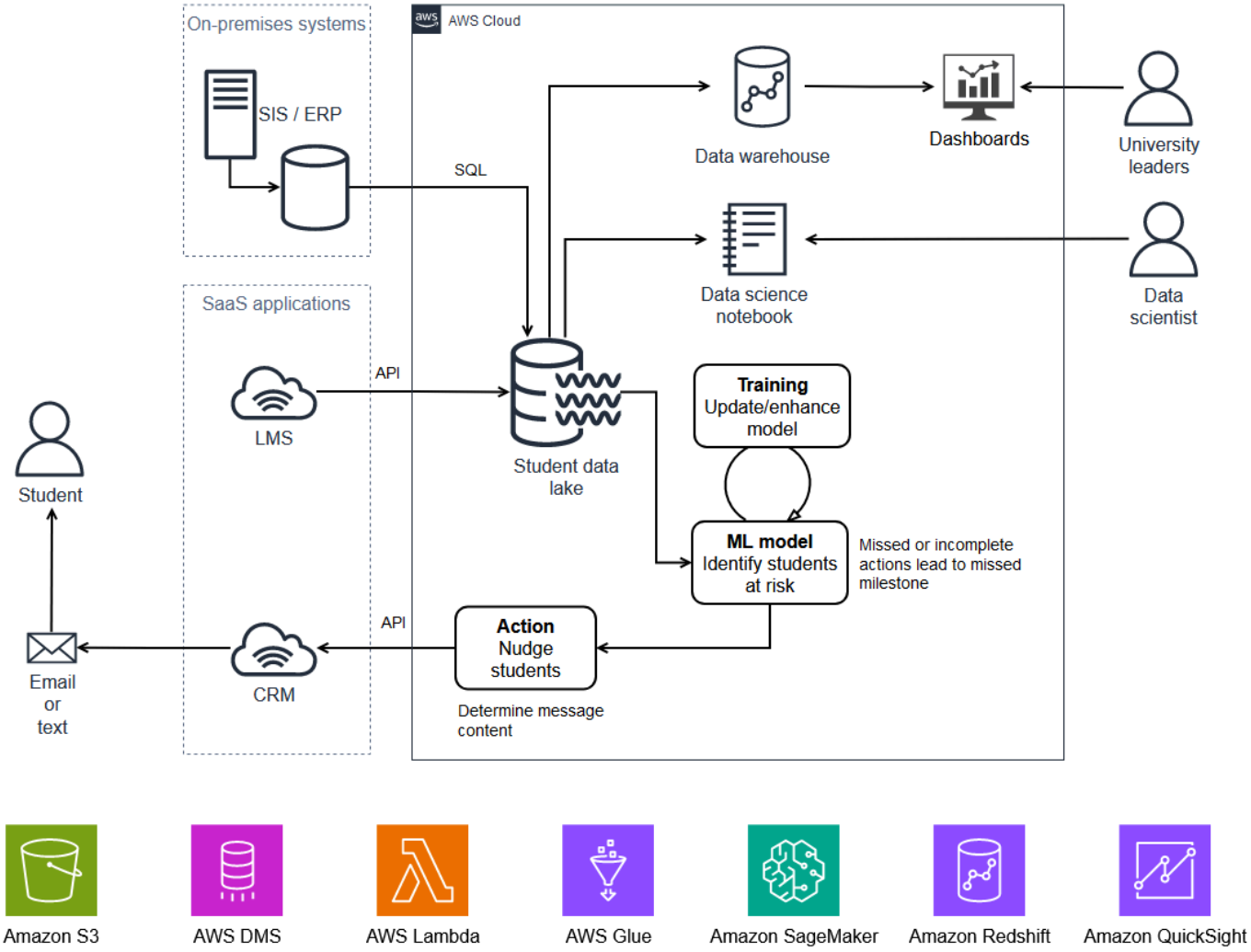
Predição do sucesso estudantil

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:

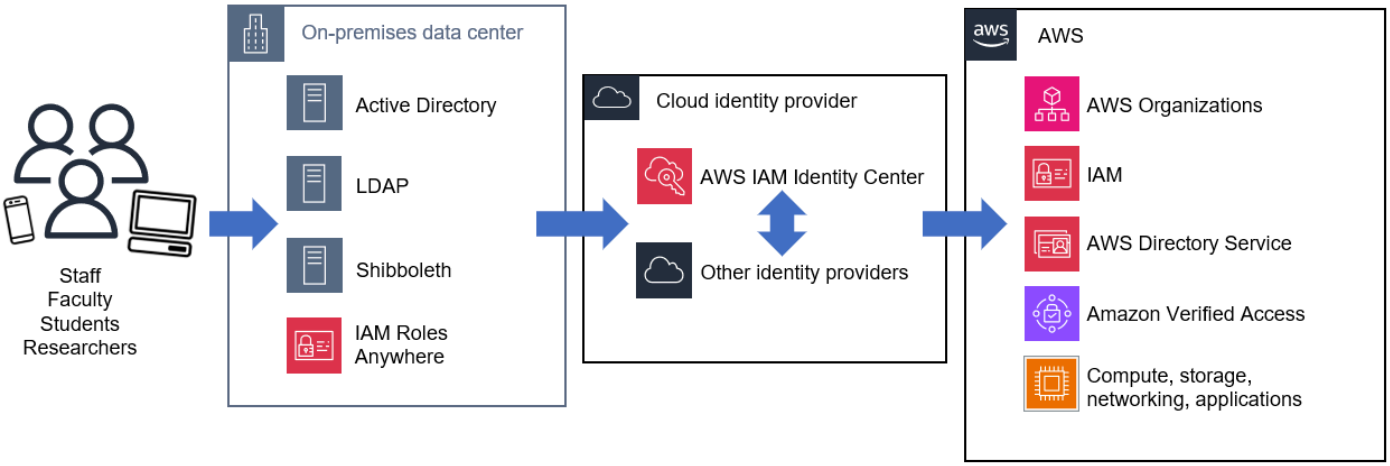
- Selecione um provedor de nuvem primário e estratégico.O provedor estratégico de nuvem da universidade hospeda toda a solução implantada. Isso permite que a equipe de TI e de negócios se concentre no desenvolvimento de habilidades em um único conjunto integrado de recursos de nuvem.
- Diferencie entre 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 possível e prático. Cloud-native os serviços gerenciados 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 de ponta a ponta.

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 de gerenciamento de identidades robustas e fáceis de integrar que permitam federar identidades por meio de provedores de identidade em nuvem para suas aplicações 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

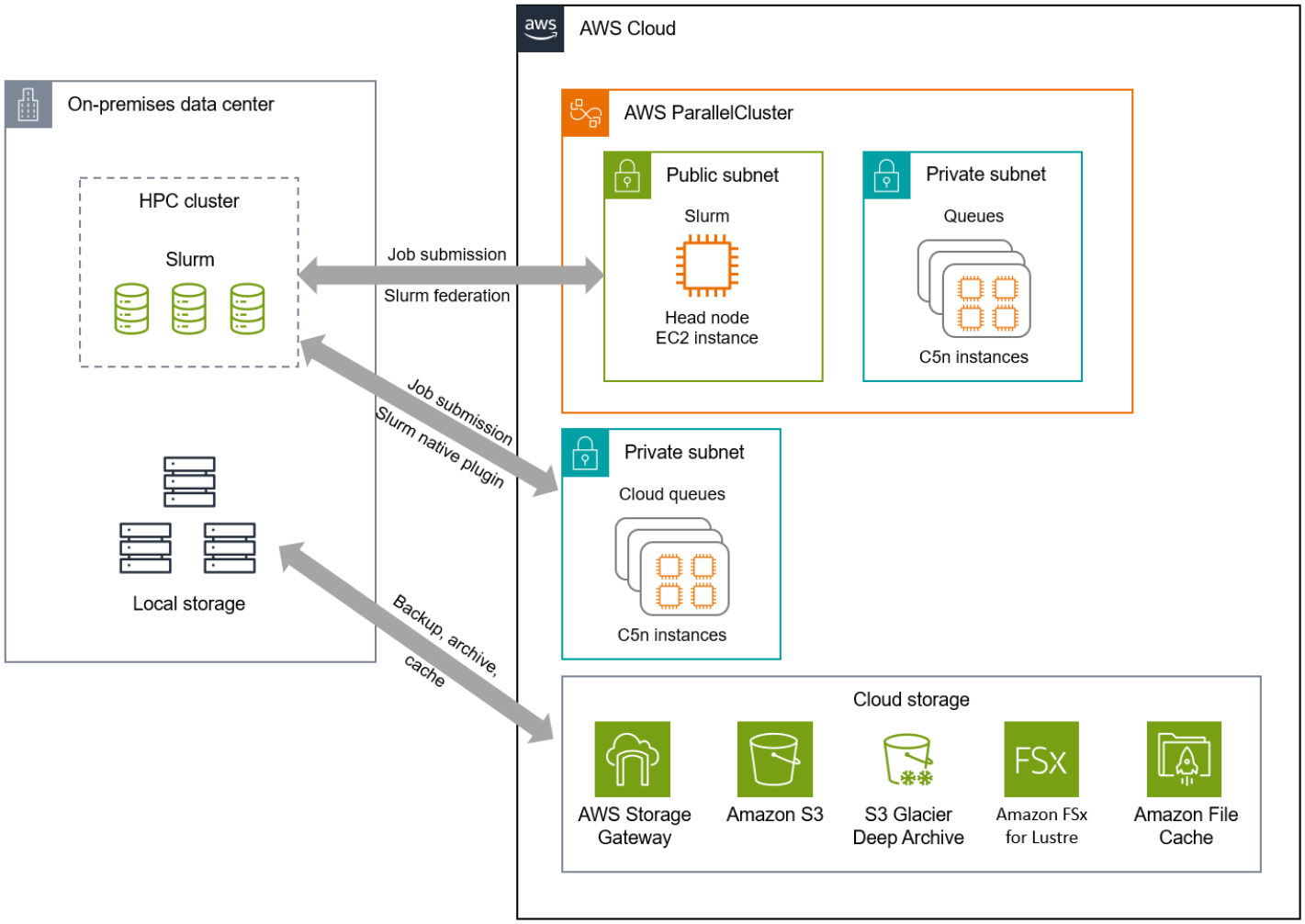
O grupo de computação de pesquisa de uma instituição de pesquisa R1 (Doctoral Universities – Very High Research Activity) nos EUA já executava clusters de computação de alta performance (HPC) on-premises com o agendador Slurm há muitos anos. Com exceção de algumas semanas de manutenção programada, os 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 aprendizado de máquina (AI/ML) para previsão do tempo, mas exigia mais capacidade do que a disponível. O grupo de computação de pesquisa também estava recebendo mais solicitações para as unidades de processamento gráfico (GPUs) mais recentes para treinar modelos de machine learning. Mesmo com o financiamento para novas GPUs, a equipe precisaria esperar meses para obter aprovação para expandir o espaço em racks 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

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.