Escolhendo a abordagem de acesso certa para a Amazon QuickSight

AWS Orientação prescritiva

AWS Orientação prescritiva: Escolhendo a abordagem de acesso certa para a Amazon QuickSight

Table of Contents

Escolhendo a abordagem de acesso certa para a Amazon QuickSight

Henry Kong, Amazon Web Services (AWS)

Maio de 2024 (histórico do documento)

QuickSightA Amazon é um serviço de inteligência de negócios (BI) em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em painéis. O acesso à maioria Serviços da AWS é configurado por meio de AWS Identity and Access Management (IAM) e políticas. Você pode configurar o acesso QuickSight usando o IAM ou usar uma das outras abordagens disponíveis que podem ser configuradas diretamente no serviço, como usuários locais, federação e integração de diretórios. Para a maioria dos casos de uso, AWS IAM Identity Center é a forma recomendada de gerenciar o QuickSight acesso. Este guia descreve as opções disponíveis para provisionar o acesso para QuickSight que você possa selecionar a opção apropriada para sua organização. Ele também discute casos de uso e fatores de configuração e operações que podem influenciar essa decisão.

Resultados de negócios desejados

Este guia pode ajudar você e sua organização a alcançar os seguintes objetivos:

- Entenda as diferentes abordagens para gerenciar o acesso do usuário ao QuickSight
- Identifique os vários recursos de acesso QuickSight que são importantes para sua organização e se alinhem melhor aos seus processos e casos de uso
- Tome uma decisão informada sobre qual abordagem de QuickSight acesso é a melhor para sua organização

Público-alvo

Este guia é destinado a arquitetos corporativos, arquitetos de dados e arquitetos de identidade e acesso que estão tomando decisões técnicas estratégicas sobre o uso de QuickSight dentro de sua organização.

Visão geral das abordagens

Embora existam muitas abordagens diferentes que podem ser usadas para gerenciar o acesso à Amazon QuickSight, a abordagem recomendada é usar a AWS IAM Identity Center integração. Em alguns casos, uma abordagem diferente pode ser considerada se você tiver requisitos específicos que são discutidos mais detalhadamente neste guia.

Você pode usar as seguintes abordagens para configurar o acesso a QuickSight:

- Integração com o Centro de Identidade do IAM— Use a integração de serviços integrada entre QuickSight o IAM Identity Center, um recurso lançado em agosto de 2023. Essa abordagem requer a edição Enterprise do QuickSight.
- Usuários federados— Gerencie usuários com um provedor de identidade corporativa (IdP) para autenticar os usuários quando eles fizerem login. QuickSight
- Usuários do Active Directory— Conceda acesso a um grupo de diretórios no Microsoft Active Directory. Essa abordagem requer a edição Enterprise do QuickSight. As seguintes opções estão disponíveis:
  - AWS Directory Service for Microsoft Active Directory
  - AD Connector apontando para AWS Managed Microsoft AD
  - AD Connector apontando para um diretório autogerenciado
- usuários do IAM— Conceda acesso para usuários existentes AWS Identity and Access Management (IAM). As seguintes opções estão disponíveis:
  - Envie aos usuários do IAM um convite por e-mail
  - Conceda aos usuários ou grupos de usuários do IAM permissões para autoprovisionamento
- QuickSight usuários— Crie usuários locais dentro QuickSight.

Há muitas opções para escolher ao configurar o acesso do usuário a. QuickSight Ao compreender as vantagens e limitações de cada abordagem, você pode determinar a abordagem correta para sua organização. Também é possível adotar mais de uma abordagem para sua organização, dependendo de determinadas circunstâncias. No entanto, isso aumenta a complexidade das operações de provisionamento.

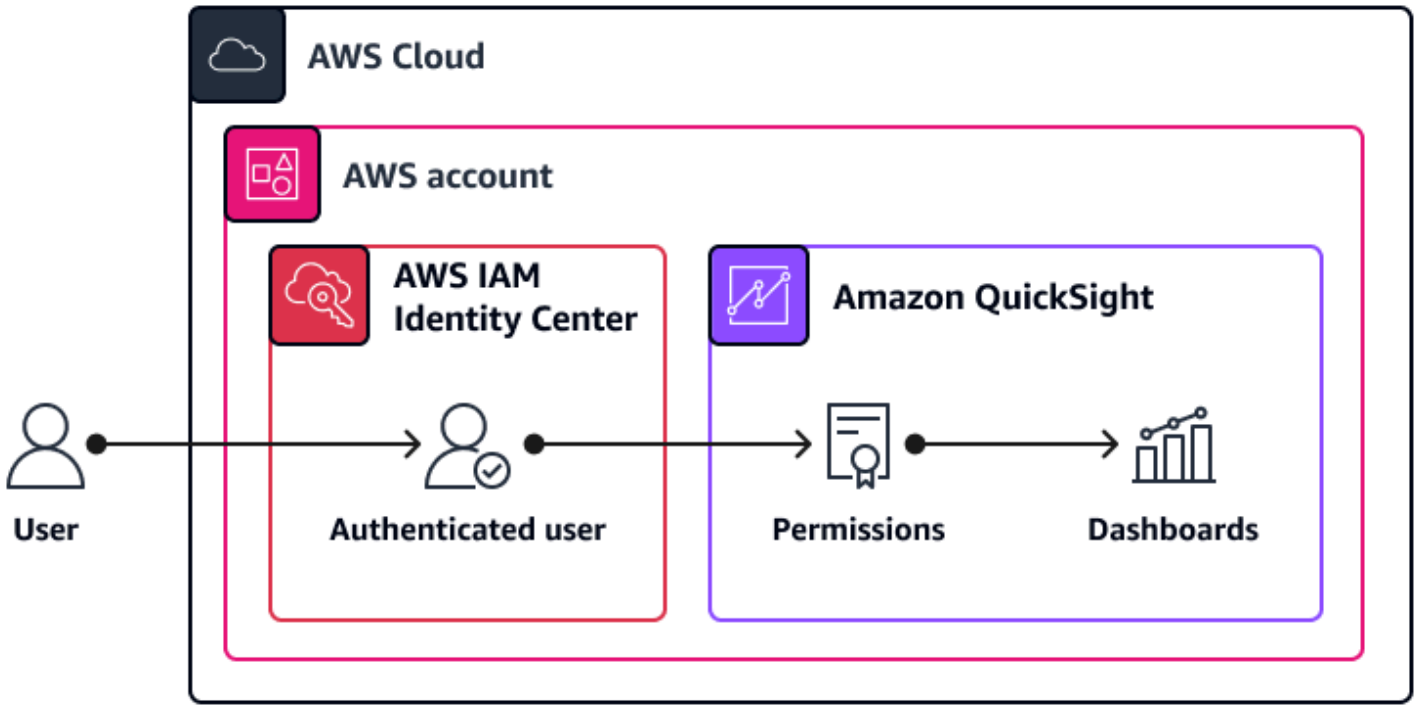
Diferenças entre as QuickSight edições

As opções de gerenciamento de acesso variam entre as edições Standard e Enterprise do QuickSight. A tabela a seguir compara as opções de acesso de cada uma. Para obter mais informações, consulte Gerenciamento de usuários entre edições na QuickSight documentação.

Abordagem de acesso	Standard Edition	Enterprise Edition
QuickSight usuário	Sim	Sim
IAM user (Usuário do IAM)	Sim	Sim
Usuário do Active Directory	Não	Sim
Integração com o Centro de Identidade do IAM	Não	Sim
Usuário federado	Sim	Sim

Conceder QuickSight acesso por meio da integração com o IAM Identity Center

> **Note**
>
> Essa abordagem de acesso está disponível somente para a edição Enterprise da Amazon QuickSight. Para obter mais informações, consulte Gerenciamento de usuários para a edição Enterprise na QuickSight documentação.



A seguir estão as características dessa arquitetura e abordagem de acesso:

- Usuários e grupos são gerenciados AWS IAM Identity Center por meio de uma das seguintes fontes de identidade:
  - Um provedor de identidade externo
  - Um diretório do Microsoft Active Directory
  - Um diretório do IAM Identity Center
- Dependendo dos seus requisitos, você pode usar uma instância da organização ou uma instância de conta do IAM Identity Center. Por exemplo, se os usuários externos precisarem acessar,

QuickSight mas não estiverem disponíveis ou não tiverem permissão para serem provisionados na instância da organização, você poderá usar uma instância de conta que use uma fonte de identidade compatível com usuários internos e externos.

- Você atribui acesso de QuickSight administrador, autor ou leitor aos grupos do IAM Identity Center.
- QuickSight o acesso é provisionado com base nas associações mapeadas do grupo do IAM Identity Center.
- Você não pode combinar essa abordagem de QuickSight acesso com outras abordagens.

Considerações e casos de uso

É recomendável usar o IAM Identity Center para gerenciar o acesso QuickSight a. Há duas abordagens que você pode usar com o IAM Identity Center. QuickSight é um aplicativo habilitado para o IAM Identity Center e oferece suporte à integração nativa, que é a abordagem recomendada. Também é possível usar a federação SAML 2.0, conforme descrito Configurando o acesso de usuários federados QuickSight por meio do IAM Identity Center neste guia, mas essa abordagem não é recomendada para a maioria dos casos de uso.

A integração de serviços nativos entre o IAM Identity Center QuickSight e o IAM não exige a configuração da federação SAML entre os dois serviços. A integração nativa usa associações de grupos do IAM Identity Center para gerenciar o acesso a. QuickSight

Os grupos de usuários do IAM Identity Center são sincronizados automaticamente com QuickSight. No QuickSight console, os administradores podem mapear os grupos do IAM Identity Center para as QuickSight funções. Os grupos podem receber as funções Admin, Author, Reader, Admin Pro, Author Pro ou Reader Pro.

Essa abordagem é útil porque não exige que você mantenha a configuração da federação ou qualquer conjunto de permissões. No entanto, depois que essa abordagem for implementada, você não poderá mudar para uma abordagem diferente, como federação, no futuro, sem encerrar sua QuickSight assinatura. Você também não pode combinar essa abordagem com outras abordagens.

Para outras limitações relacionadas ao uso da integração QuickSight nativa com o IAM Identity Center, consulte a QuickSightdocumentação. Por exemplo, o uso do recurso de namespaces no não QuickSight é suportado se você usar a integração do IAM Identity Center.

Pré-requisitos

- Um ativo Conta da AWS
- As seguintes permissões:
  - Acesso administrativo ao “ Conta da AWS onde QuickSight está inscrito”
  - Acesso ao console do IAM Identity Center para atribuir usuários a grupos

Configurando a integração e o acesso do usuário ao IAM Identity Center

Observe o seguinte ao configurar esse tipo de acesso:

1. Antes de se inscrever QuickSight, verifique se você já configurou e configurou o IAM Identity Center. Para obter instruções, consulte os tutoriais de ativação AWS IAM Identity Center e introdução na documentação do IAM Identity Center.
2. Siga as instruções em Inscrever-se para uma QuickSight assinatura na QuickSight documentação. Escolha Enterprise e, em seguida, escolha Usar aplicativo habilitado para o IAM Identity Center. Dependendo de quais instâncias existentes do IAM Identity Center estão disponíveis na sua Conta da AWS, você pode selecionar entre uma instância da organização ou uma instância da conta.
3. Para atribuir QuickSight funções aos grupos do IAM Identity Center, siga as instruções em Gerenciando o acesso para usuários do IAM Identity Center na QuickSight documentação.

Concedendo QuickSight acesso a usuários federados

Ao usar identidades federadas, você pode gerenciar usuários com um provedor de identidade externo (IdP) para autenticar os usuários quando eles fazem login na Amazon. QuickSight QuickSight oferece suporte à federação de identidades com o SAML 2.0. Muitos externos IdPs, como Okta e Ping, usam esse padrão. Você também pode usar AWS IAM Identity Center como seu IdP externo para acessar uma abordagem de federação SAML 2.0. QuickSight No entanto, recomendamos a integração de serviços incorporada discutida Integração com o Centro de Identidade do IAM neste guia, em vez da abordagem de usuário federado. Se você usa o IAM Identity Center, a abordagem de usuário federado só é recomendada se você não puder usar a integração do IAM Identity Center devido às limitações atuais dos recursos.

Os usuários federados têm uma experiência de login único (SSO), e você pode conceder acesso QuickSight sem criar um usuário AWS Identity and Access Management (IAM) ou usuário QuickSight local para cada pessoa em sua organização. Além disso, a federação fornece aos usuários credenciais temporárias, o que é uma prática recomendada de segurança. Para obter mais informações sobre a federação de identidades e seus benefícios e casos de uso, consulte Federação de identidades em AWS.

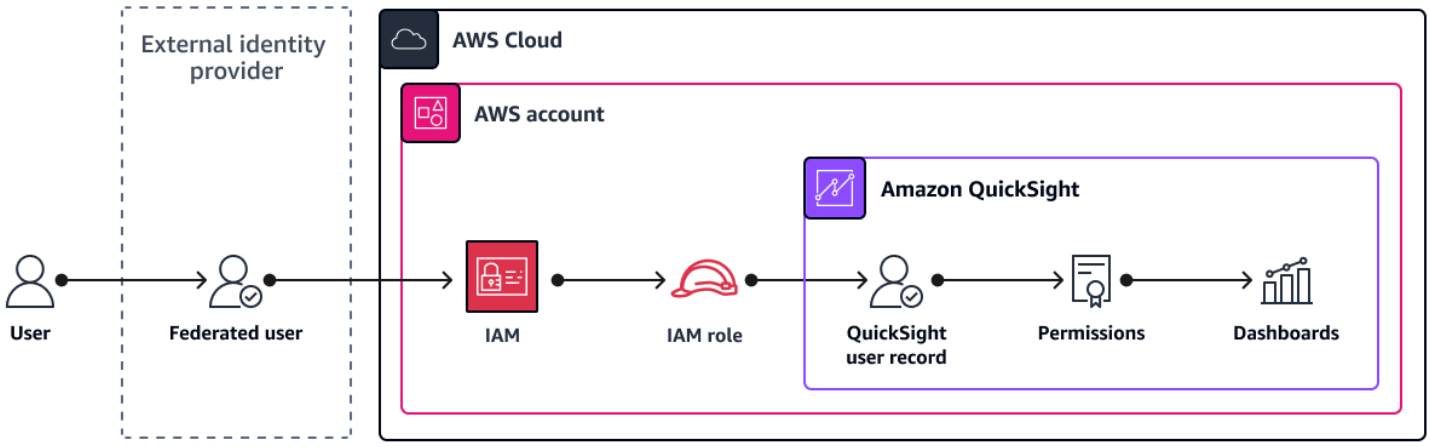
Ao configurar o acesso QuickSight para usuários federados, você pode usar uma das seguintes abordagens:

- Configurando o acesso de usuários federados QuickSight por meio do IAM e de um IdP externo
- Configurando o acesso de usuários federados QuickSight por meio do IAM Identity Center

Ambas as abordagens permitem que usuários federados provisionem automaticamente o acesso a. QuickSight As abordagens variam com base na arquitetura e nos serviços usados para federação. No entanto, em ambas as soluções, o usuário federado assume então uma função do IAM que determina quais permissões ele tem. QuickSight

Ao usar a edição QuickSight Enterprise, você pode forçar os usuários que estão autoprovisionando seu acesso a se conectarem QuickSight usando o endereço de e-mail definido no provedor de identidade. Para ter mais informações, consulte QuickSight sincronização de e-mail para usuários federados.

Configurando o acesso de usuários federados QuickSight por meio do IAM e de um IdP externo



A seguir estão as características dessa arquitetura:

- O registro de QuickSight usuário da Amazon está vinculado a uma função AWS Identity and Access Management (IAM) e ao nome de usuário no IdP, como. `QuickSightReader/DiegoRamirez@example.com`
- Os usuários podem autoprovisionar o acesso.
- Os usuários fazem login em seu provedor de identidade externo.
- Se a sincronização de e-mail estiver desativada, os usuários poderão fornecer seu endereço de e-mail preferido ao QuickSight entrarem. Se a sincronização de e-mail estiver ativada, QuickSight usa o endereço de e-mail definido no IdP corporativo. Para obter mais informações, consulte QuickSight sincronização de e-mail para usuários federados neste guia.
- A função do IAM contém uma política de confiança que permite que somente usuários federados do seu IdP externo assumam a função.

Considerações e casos de uso

Se você já usa a federação de identidades para acessar sua Contas da AWS, você pode usar essa configuração existente para também estender o acesso QuickSight a. Para QuickSight acessar, você pode reutilizar os mesmos processos que você tem em vigor para provisionar e revisar o acesso a. Contas da AWS

Pré-requisitos

- Permissões administrativas em QuickSight.
- Sua organização já está usando um provedor de identidade externo, como Okta ouPing.

Configurar o acesso

Para obter instruções, consulte Como configurar a federação de IdP usando o IAM e QuickSight na QuickSight documentação. Para obter mais informações sobre como configurar a política de permissões para QuickSight, consulte Configurar políticas do IAM este guia.

Configurando o acesso de usuários federados QuickSight por meio do IAM Identity Center

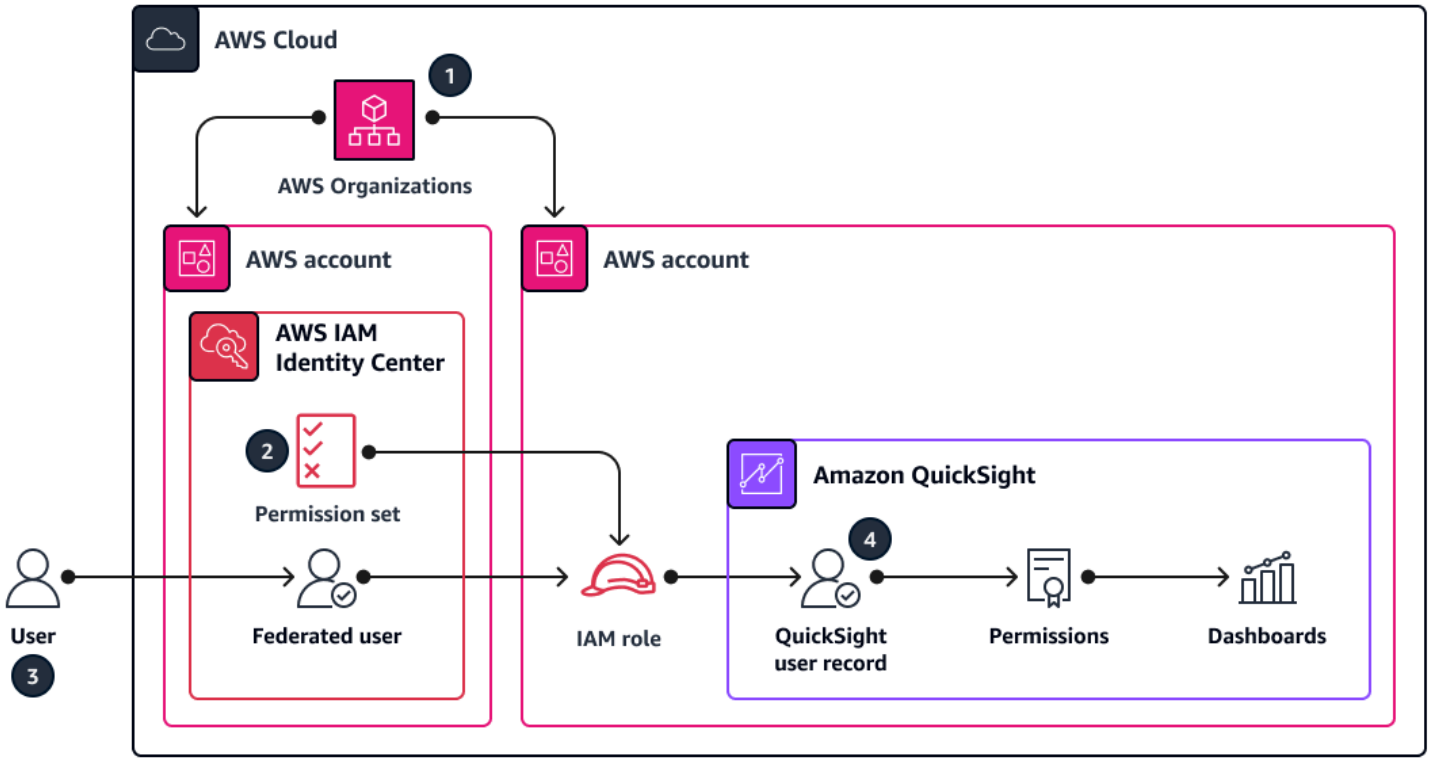
Se sua empresa já estiver usando AWS IAM Identity Center, talvez você queira usar esse serviço para autenticar usuários federados. Você pode usar a federação SAML 2.0 ou usar a integração de serviços integrada entre o IAM Identity Center. Para obter mais informações sobre a integração de serviços incorporada, consulte Integração com o Centro de Identidade do IAM este guia.

Ao usar a federação SAML 2.0 com o IAM Identity Center, há dois métodos para configurar o acesso do usuário federado a: QuickSight

- Configurando permissões usando conjuntos de permissões— Você pode usar essa abordagem somente se Contas da AWS for do IAM Identity Center e QuickSight for membro da mesma organização em AWS Organizations. Um conjunto de permissões é um modelo que define uma coleção de uma ou mais políticas AWS Identity and Access Management (IAM). Os conjuntos de permissões podem simplificar o gerenciamento de permissões em sua organização.
- Configurando permissões usando funções do IAM— Essa abordagem é adequada se o Conta da AWS QuickSight for não fizer parte da mesma organização do IAM Identity Center. Nessa abordagem, você cria as funções do IAM diretamente na mesma conta com QuickSight.

Em ambas as abordagens, os usuários podem autoprovisionar seu próprio QuickSight acesso. Se a sincronização de e-mail estiver desativada, os usuários poderão fornecer seu endereço de e-mail preferido ao QuickSight entrarem. Se a sincronização de e-mail estiver ativada, QuickSight usa o endereço de e-mail definido no IdP corporativo. Para obter mais informações, consulte QuickSight sincronização de e-mail para usuários federados neste guia.

Configurando permissões usando conjuntos de permissões



A seguir estão as características dessa arquitetura e abordagem de acesso:

1. Contas da AWS Para o IAM Identity Center e QuickSight estão na mesma organização em AWS Organizations.
2. O conjunto de permissões que você define no IAM Identity Center gerencia e controla a função do IAM.
3. Os usuários fazem login por meio do IAM Identity Center.
4. O registro QuickSight do usuário está vinculado à função do IAM gerenciada pelo IAM Identity Center e ao nome de usuário, como`AWSReservedSSO_QuickSightReader_7oe58cd620501f23/DiegoRamirez@example.com`.

Pré-requisitos

- Uma QuickSight conta ativa
- As seguintes permissões:
  - Acesso do administrador ao “ Conta da AWS onde QuickSight está inscrito”

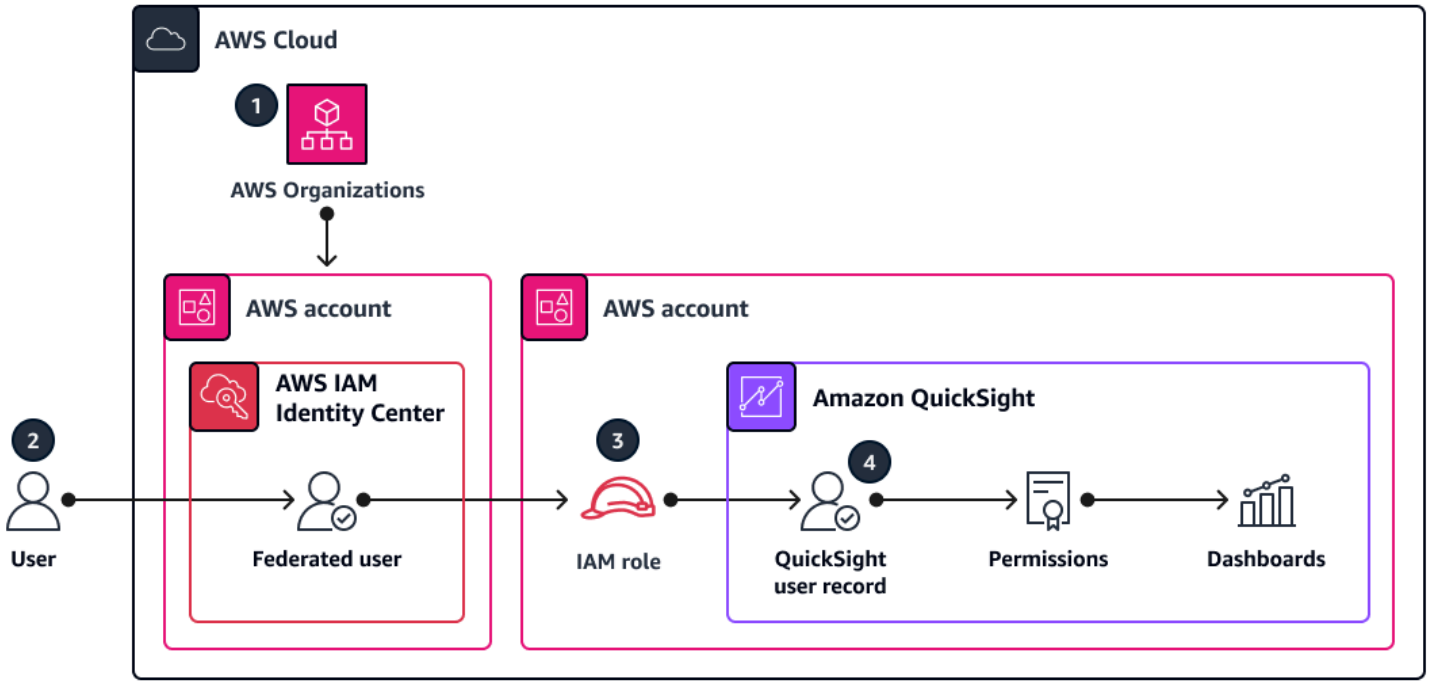
- Acesso ao console do IAM Identity Center e permissões para criar conjuntos de permissões

Configurar o acesso

Antes de se inscrever QuickSight, verifique se você já configurou e configurou o IAM Identity Center. Para obter instruções, consulte os tutoriais de ativação AWS IAM Identity Center e introdução na documentação do IAM Identity Center. Depois de configurar o IAM Identity Center em sua organização, crie um conjunto de permissões personalizado no IAM Identity Center que permita o acesso QuickSight de usuários federados. Para obter instruções, consulte Criar um conjunto de permissões na documentação do IAM Identity Center. Para obter mais informações sobre como configurar as políticas que você inclui no conjunto de permissões, consulte Configurar políticas do IAM este guia.

Depois de criar o conjunto de permissões, provisione-o para o destino Conta da AWS em que QuickSight está inscrito e, em seguida, aplique-o aos usuários e grupos que precisam de QuickSight acesso. Para obter mais informações sobre a atribuição de conjuntos de permissões, consulte Atribuir acesso ao usuário Contas da AWS na documentação do IAM Identity Center.

Configurando permissões usando funções do IAM



A seguir estão as características dessa arquitetura e abordagem de acesso:

1. Eles Contas da AWS são do IAM Identity Center e não QuickSight estão na mesma organização em AWS Organizations.
2. Os usuários fazem login por meio do IAM Identity Center ou por meio do IdP externo que você configurou como fonte de identidade no IAM Identity Center.
3. A função do IAM contém uma política de confiança que permite que somente usuários federados do IAM Identity Center assumam a função.
4. O registro QuickSight do usuário está vinculado a uma função do IAM e ao nome de usuário no IdP, como. `QuickSightReader/DiegoRamirez@example.com`

Pré-requisitos

- Uma QuickSight conta ativa.
- As seguintes permissões:
  - O acesso do administrador ao Conta da AWS onde QuickSight está inscrito.
  - Acesso ao console do IAM Identity Center e permissões para gerenciar aplicativos.
- Você configurou e configurou o IAM Identity Center. Para obter instruções, consulte os tutoriais de ativação AWS IAM Identity Center e introdução na documentação do IAM Identity Center.
- Você configurou o IAM Identity Center como um IdP confiável no IAM. Para obter instruções, consulte Criação de provedores de identidade do IAM na documentação do IAM.

Configurar o acesso

Para obter instruções, consulte o Guia de AWS IAM Identity Center integração da Amazon QuickSight. Depois de configurar o IAM Identity Center como um provedor de identidade confiável para o Conta da AWS, crie uma função do IAM que os usuários federados possam assumir para acessar QuickSight. Para obter instruções, consulte Como criar funções do IAM na documentação do IAM. Para obter mais informações sobre como configurar as políticas para QuickSight, consulte Configurar políticas do IAM este guia.

QuickSight sincronização de e-mail para usuários federados

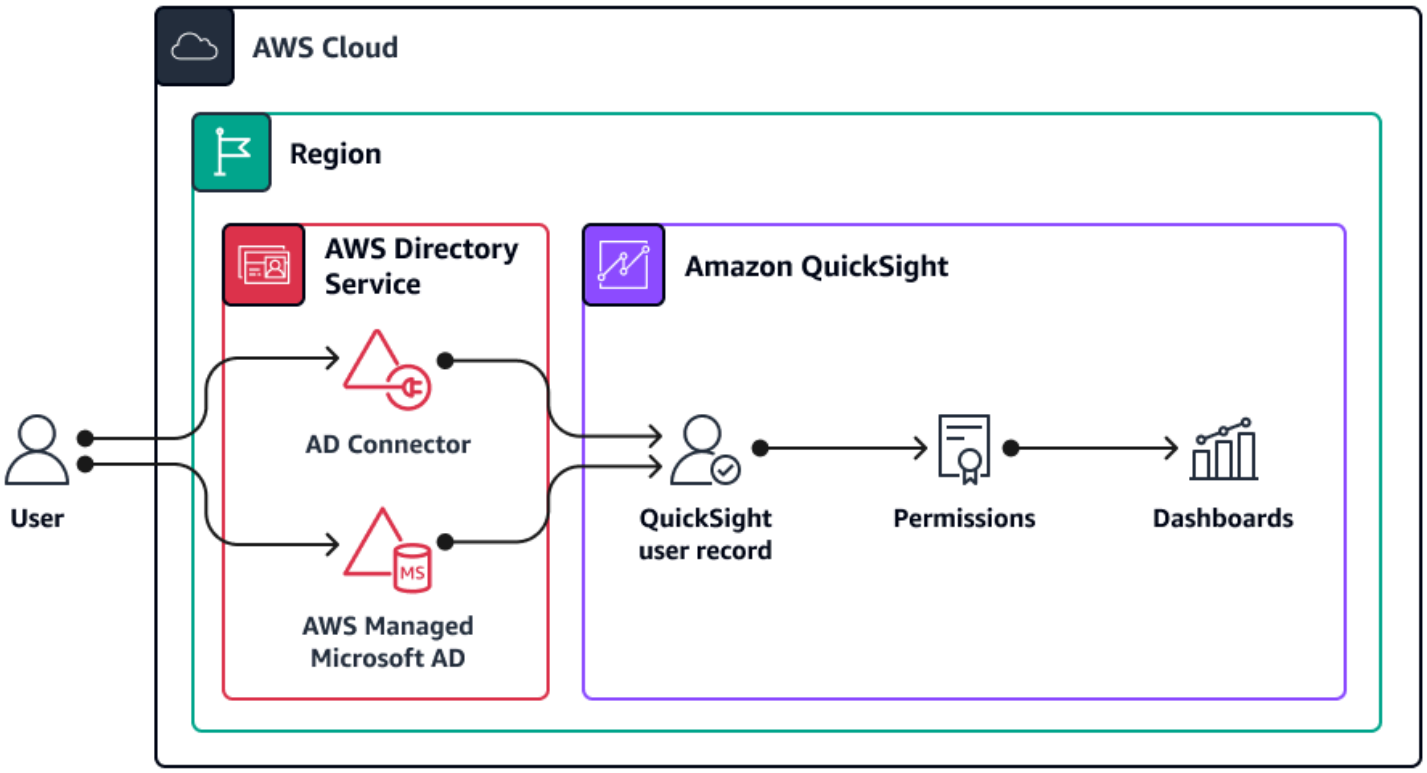
> **Note**
>
> Esse recurso está disponível somente para a edição Enterprise da Amazon QuickSight.

Quando os usuários do IAM fornecem acesso por conta própria QuickSight, os administradores não conseguem controlar qual endereço de e-mail o usuário fornece. QuickSight Os usuários poderiam inserir um endereço de e-mail pessoal em vez do endereço de e-mail profissional. Isso pode não ser aceitável para algumas organizações. No entanto, quando você está usando um provedor de identidade para fornecer acesso federado à edição QuickSight Enterprise, QuickSight tem um recurso que garante que o endereço de e-mail do usuário QuickSight corresponda ao endereço de e-mail do usuário no provedor de identidade.

No IdP, você adiciona um atributo SAML para o endereço de e-mail do usuário. O processo de criação do atributo ou token é diferente para cada IdP. Veja as instruções do Okta ou do IAM Identity Center ou consulte a documentação do IdP da sua organização. O IdP passa o e-mail do usuário como uma tag de `Principal` sessão do IAM. QuickSight usa essa tag de sessão em vez de solicitar que o usuário forneça seu endereço de e-mail. Para obter instruções sobre como habilitar esse recurso, consulte Configurando a sincronização de e-mail para usuários federados na documentação. QuickSight

Concedendo QuickSight acesso aos usuários do Active Directory

> **Note**
>
> Essa abordagem de acesso está disponível somente para a edição Enterprise da Amazon QuickSight. Para obter mais informações, consulte Gerenciamento de usuários para a edição Enterprise na QuickSight documentação.



A seguir estão as características dessa arquitetura e abordagem de acesso:

- O registro QuickSight do usuário da Amazon está vinculado ao usuário no Active Directory.
- Você atribui acesso de QuickSight administrador, autor ou leitor aos grupos do Active Directory.
- QuickSight o acesso é provisionado com base nas associações mapeadas do grupo do Active Directory.
- As senhas de usuário são gerenciadas no Active Directory.

- O usuário deve fazer login diretamente pelo QuickSight console em https://quicksight.aws.amazon.com/.
- Você não pode combinar essa abordagem de QuickSight acesso com outras abordagens.

Considerações e casos de uso

Você pode usar usuários e grupos do Microsoft Active Directory para gerenciar o acesso QuickSight a. QuickSight suporta o AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) ou o Conector do Active Directory (AD Connector).

AWS Managed Microsoft AD é um host do Active Directory Nuvem AWS que oferece a maioria das mesmas funcionalidades do Active Directory. Se você tiver um diretório autogerenciado existente para o qual deseja usar QuickSight, poderá usar o AD Connector. Esse serviço redireciona as solicitações de diretório para seu Active Directory autogerenciado, em outro local Região da AWS ou no local, sem armazenar nenhuma informação em cache na nuvem. Tanto o AD Connector quanto o AD AWS Managed Microsoft AD fazem parte do AWS Directory Service.

Seu diretório ou conexão de diretório AWS Directory Service deve estar no mesmo em Região da AWS que você está se inscrevendo QuickSight. Ao se inscrever QuickSight, você especifica o domínio do Active Directory, bem como os grupos específicos do Active Directory que serão usados para controle de acesso.

Essa abordagem de acesso é mais adequada para organizações que desejam usar seus processos existentes de gerenciamento de acesso do Active Directory. Essa abordagem gerencia o QuickSight acesso e as funções por meio de associações a grupos do Active Directory.

Uma consideração importante ao usar essa abordagem é que ela não pode ser combinada com outras abordagens. Por exemplo, você pode criar uma abordagem de acesso híbrido usando usuários do IAM e usuários QuickSight locais. Considere essa abordagem com cuidado. Se você selecionar essa abordagem ao configurar QuickSight, estará se comprometendo com ela. Você não pode mudar para uma abordagem diferente posteriormente.

Essa não é a única abordagem de acesso que usa o Active Directory. Nessa abordagem, o QuickSight acesso é provisionado com base na associação ao grupo no Active Directory, e o registro do QuickSight usuário é vinculado diretamente ao usuário do Active Directory. Você também pode usar o Active Directory como fonte de identidade para federação de usuários. Para obter mais informações, consulte Usuários federados neste guia.

Pré-requisitos

- Edição corporativa do QuickSight
- Permissões para assinar QuickSight, criar usuários e gerenciar o Active Directory (consulte as políticas baseadas em identidade do IAM para a Amazon QuickSight: acesso total à edição Enterprise)

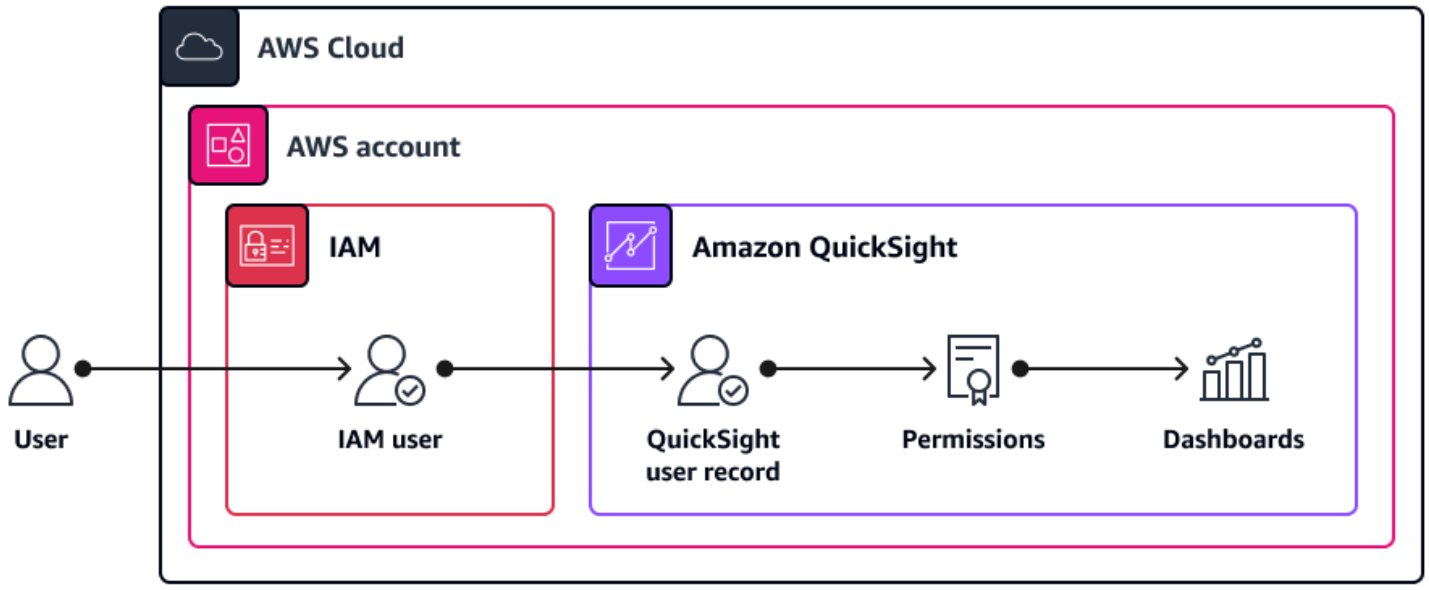
Configurando o acesso para usuários do Active Directory

Depois de confirmar os detalhes do seu diretório, você pode se inscrever no QuickSight. Para obter instruções, consulte Inscrever-se para uma QuickSight assinatura. Observe o seguinte ao configurar esse tipo de acesso:

1. No assistente de QuickSight inscrição, escolha Enterprise e, em seguida, escolha Usar Active Directory.
2. Vá para o QuickSight console e escolha Gerenciar acesso QuickSight a.
3. Selecione os grupos do Active Directory que devem ter QuickSight acesso e atribua a eles funções de QuickSight administrador, autor ou leitor. Para obter instruções, consulte Gerenciamento do acesso do usuário.

Conceder QuickSight acesso aos usuários do IAM

> **Note**
>
> Um usuário do IAM é uma entidade que você cria no AWS Identity and Access Management (IAM). Esse tipo de entidade acessa você Conta da AWS usando credenciais de longo prazo. Como prática recomendada, AWS recomenda que você conceda acesso por meio de credenciais temporárias usando federação de identidades e funções do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.



A seguir estão as características dessa arquitetura e abordagem de acesso:

- O registro QuickSight do usuário da Amazon está vinculado ao usuário no IAM.
- As senhas de usuário são gerenciadas no IAM.
- Você pode convidar usuários do IAM diretamente ou criar uma política baseada em identidade do IAM que permita que os usuários forneçam acesso por conta própria.
- Esse tipo de usuário pode fazer login pelo QuickSight console ou pelo AWS Management Console.

Considerações e casos de uso

Embora AWS geralmente não seja recomendável configurar o acesso por meio de usuários do IAM, outras abordagens de acesso, como federação, podem não estar disponíveis atualmente em sua organização. Muitas organizações que estão apenas começando sua jornada para a nuvem ainda não estabeleceram funções de IAM e estão trabalhando em uma arquitetura de conta única. Se sua organização usa usuários do IAM para acessar seu AWS ambiente, reaplicar essa abordagem QuickSight pode ser a abordagem mais direta e sensata até que sua organização ofereça suporte a outras abordagens.

Pré-requisitos

- Para a abordagem de convite direto, você precisa:
  - Permissões administrativas em QuickSight (consulte as políticas baseadas em identidade do IAM para as edições Standard ou Enterprise)
  - O endereço de e-mail do usuário do IAM
- Para a abordagem de acesso autoprovisionado, o usuário precisa de permissões para criar a Amazon QuickSight (consulte as políticas baseadas em identidade do IAM para a Amazon QuickSight: criação de usuários)
- O usuário do IAM deve ter uma senha associada às suas credenciais do IAM

Configurando o acesso para um usuário do IAM

Você pode conceder acesso QuickSight aos usuários do IAM usando uma das seguintes opções:

- Convite direto — Você convida o usuário do IAM para acessar QuickSight, e o usuário pode aceitar o convite por e-mail.
- Acesso autoprovisionado — você cria uma política do IAM que permite aos usuários provisionar seu próprio acesso. Quando um usuário acessa QuickSight pela primeira vez, ele recebe acesso e define o endereço de e-mail que será associado ao seu registro de QuickSight usuário.

O resultado das duas opções é o mesmo: o usuário do IAM pode acessar QuickSight. No entanto, existem vantagens e desvantagens em cada uma, conforme mostrado na tabela a seguir. Por exemplo, o convite direto pode ser preferível para organizações que desejam impor o uso de endereços de e-mail corporativos aprovados.

Abordagem	Vantagens	Desvantagens
Convite direto	• Os administradores podem controlar qual endereço de e-mail está associado ao registro do usuário no QuickSight • Sem tarefas de gerenciam ento de políticas do IAM	• Mais manual
Acesso autoprovisionado	• Pode ser integrado aos processos operacionais de TI existentes para provision ar o acesso por meio de políticas do IAM, onde o recurso de autoprovi sionamento já faz parte das políticas existentes do IAM	• Os administradores não podem controlar qual endereço de e-mail o usuário fornece para QuickSight

Convite direto

Para obter instruções sobre como configurar o acesso para um usuário do IAM, consulte Convidar usuários para acessar a Amazon QuickSight. Observe o seguinte ao configurar esse tipo de acesso do usuário:

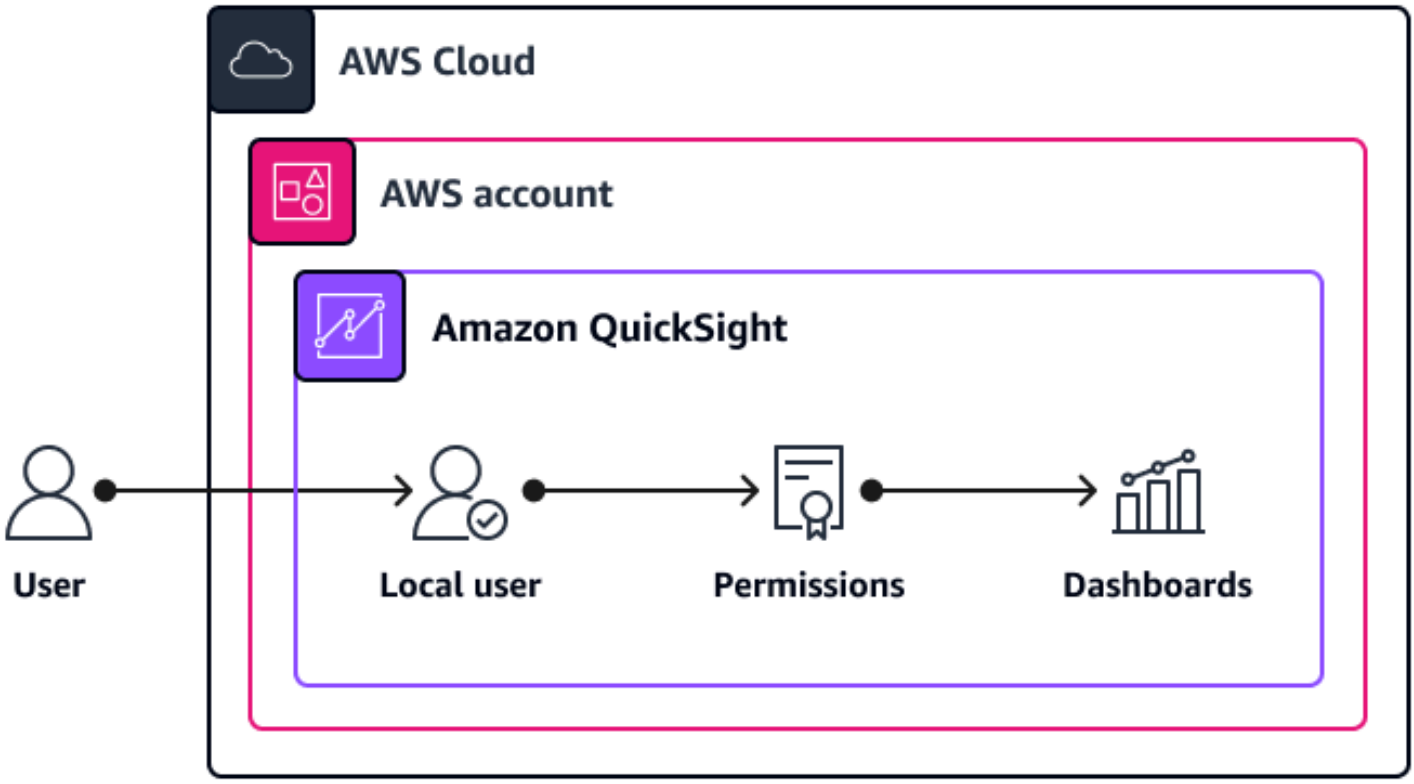
- Para o QuickSight nome de usuário, insira o nome de usuário do IAM. Os caracteres permitidos são letras, números e os seguintes caracteres:. _ - (hífen).
- Para usuário do IAM, escolha Sim.
- O usuário tem sete dias para aceitar o convite. Se eles não aceitarem dentro desse período, você poderá reenviar o e-mail de convite.
- Quando o usuário aceita o convite, ele deve inserir a senha associada às suas credenciais do IAM.

Acesso autoprovisionado

Quando os usuários do IAM podem autoprovisionar o acesso, eles não precisam ser convidados para a QuickSight conta. Na primeira vez que tentarem acessar o QuickSight console, precisarão inserir um endereço de e-mail. Quando o usuário escolhe Continuar, QuickSight cria um registro de usuário para esse usuário do IAM.

Para conceder permissão para provisionar seu próprio acesso, você cria uma política baseada em identidade e aplica essa política aos usuários do IAM ou ao grupo de usuários do IAM. Para obter mais informações, consulte Configurar políticas do IAM neste guia.

Criação de usuários locais em QuickSight



A seguir estão as características dessa arquitetura e abordagem de acesso:

- Esse usuário tem acesso QuickSight somente à Amazon e não pode acessar outros serviços e recursos no seu Conta da AWS.
- A senha do usuário é gerenciada localmente em QuickSight.
- Você fornece acesso convidando o usuário por meio de seu endereço de e-mail.
- O usuário deve fazer login diretamente pelo QuickSight console em https://quicksight.aws.amazon.com/.

Considerações e casos de uso

Essa é a maneira mais direta de provisionar o acesso, QuickSight pois ela cria um registro de usuário local dentro QuickSight do repositório de usuários e não tem dependências externas. Esse registro de usuário existe somente em QuickSight e tem uma senha que também é gerenciada em QuickSight.

Esse tipo de abordagem também é provavelmente o mais flexível porque o único pré-requisito é ter um endereço de e-mail para o usuário. Você não precisa criar e gerenciar usuários em outro serviço ou diretório, e essa pode ser uma maneira rápida de fornecer acesso para fornecedores ou parceiros terceirizados que precisam acessar seus QuickSight painéis. Essa abordagem de acesso é mais adequada para usuários que precisam de acesso QuickSight somente e não precisam de acesso a outros serviços e recursos no Conta da AWS.

Como esses são usuários locais QuickSight, as equipes de operações de TI precisam estabelecer processos dedicados para gerenciar solicitações de acesso, provisionar o acesso e revisar e auditar periodicamente o acesso. Por exemplo, eles não podem usar os processos de revisão de acesso existentes para identidades corporativas porque o registro do usuário é independente de outros sistemas de gerenciamento de identidade.

Pré-requisitos

- Permissões administrativas QuickSight ou permissões para criar QuickSight usuários (consulte as políticas baseadas em identidade do IAM para a Amazon QuickSight: criação de usuários)
- Endereço de e-mail para o usuário

Configurando o acesso para um usuário QuickSight local

Para obter instruções sobre como configurar um usuário local, consulte Convidar usuários para acessar a Amazon QuickSight. Observe o seguinte ao configurar esse tipo de acesso do usuário:

- Embora você possa definir qualquer nome de usuário e endereço de e-mail, recomendamos que você use valores consistentes com o diretório de funcionários da sua organização. Isso melhora a responsabilidade e a consistência.
- Para usuário do IAM, escolha Não.
- O usuário tem sete dias para aceitar o convite. Se eles não aceitarem dentro desse período, você poderá reenviar o e-mail de convite.
- Quando o usuário aceita o convite, ele é solicitado a definir e confirmar sua senha.

Configurando políticas do IAM para acesso QuickSight

Para obter mais informações sobre como as políticas AWS Identity and Access Management (IAM) funcionam, consulte QuickSight as políticas da Amazon (com base na identidade) na QuickSight documentação e consulte Políticas e permissões na documentação do IAM. Para exemplos de políticas para QuickSight, consulte exemplos de políticas do IAM para a Amazon QuickSight.

Observe as seguintes ações ao configurar políticas que permitem que os usuários provisionem automaticamente o acesso:

- `quicksight:CreateReader`permite que um usuário provisione automaticamente o acesso somente de leitura no. QuickSight Para obter mais informações, consulte Autoprovisionamento de um usuário somente para leitura da Amazon QuickSight .
- `quicksight:CreateUser`permite que um usuário forneça automaticamente o acesso do autor em QuickSight. Para obter mais informações, consulte Autoprovisionamento de um autor da Amazon. QuickSight
- `quicksight:CreateAdmin`permite que um usuário provisione automaticamente o acesso administrativo em QuickSight. Para obter mais informações, consulte Autoprovisionamento de um administrador da Amazon. QuickSight

Conclusão

Este guia analisa várias abordagens diferentes que você pode usar para provisionar o acesso do usuário à Amazon QuickSight. Em alguns casos, você pode até mesmo combinar mais de uma abordagem para oferecer suporte a diferentes casos de uso. No entanto, cada abordagem adicional aumenta a complexidade.

Se todas as opções forem possíveis para sua implantação, a abordagem recomendada é usar a integração AWS IAM Identity Center integrada com QuickSight. Para analisar essa abordagem com mais detalhes e determinar se alguma das limitações de recursos atuais se aplica à sua situação, consulte Configurar sua QuickSight conta da Amazon com o IAM Identity Center na QuickSight documentação.

Ao escolher uma abordagem, considere como ela afetará a experiência de login do usuário, a segurança e como apoiá-la com operações e processos de gerenciamento de acesso em sua organização. Mudar para uma abordagem diferente no futuro pode ser caro, ou talvez não seja possível. Antes de configurar QuickSight, reserve o tempo necessário para avaliar o que é melhor para sua organização.

Recursos

AWS service (Serviço da AWS) documentação

- AWS IAM Identity Center documentação
  - Conceitos básicos
  - Crie um conjunto de permissões
- QuickSightDocumentação da Amazon
  - Configure sua QuickSight conta da Amazon com o IAM Identity Center
  - Usando a Amazon QuickSight com o IAM
  - Exemplos de políticas do IAM para a Amazon QuickSight
  - Autoprovisionamento de usuários para a Amazon QuickSight
  - Usando federação de identidades e login único com a Amazon QuickSight
  - Usando o Active Directory com a edição Amazon QuickSight Enterprise
  - Configurando a sincronização de e-mail para usuários federados na Amazon QuickSight
  - Tutorial: Acessando a Amazon QuickSight usando Okta
- AWS Identity and Access Management Documentação (IAM)
  - Visão geral do gerenciamento de AWS identidades
  - Provedores de identidade e federação
  - Criação de provedores de identidade do IAM
  - Criação de uma função para um provedor de identidade terceirizado (federação)

Outros AWS recursos

- Federação de identidade em AWS
- Simplifique o gerenciamento de identidade de business intelligence com a Amazon QuickSight e AWS IAM Identity Center (postagem AWS no blog)

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
AWS IAM Identity Center integração	Adicionamos a seção Como conceder QuickSight acesso por meio da integração do IAM Identity Center.	14 de maio de 2024
Publicação inicial	—	18 de maio 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: migre seu banco de dados Oracle local para a edição compatível com Amazon Aurora PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape)]:: mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Amazon Relational Database Service (AmazonRDS) for Oracle no. Nuvem AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migre seu sistema de gerenciamento de relacionamento com o cliente (CRM) para a Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Oracle em uma EC2 instância no. Nuvem AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma local para um serviço em nuvem para a mesma plataforma. Exemplo: Migrar um Microsoft Hyper-V aplicativo para AWS.
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.

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

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja a inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para 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 baseado em atributos () 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 a documentação AWS Identity and Access Management (IAM). AWS

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.

Availability Zone (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 CAForganiza 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, 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 AWS CAFsite e o AWS CAFwhitepaper.

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 WQFestá incluído com AWS

Schema Conversion Tool (AWS SCT). Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

B

bot ruim

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

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

Redes de bots infectadas por malware e sob o controle de uma única parte, conhecidas como pastor de bots ou operador de bots. As redes de bots são o mecanismo mais conhecido para escalar bots e seu impacto.

ramo

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

acesso em vidro quebrado

Em circunstâncias excepcionais e por meio de um processo aprovado, um meio rápido para um usuário obter acesso a um Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador Implementar procedimentos de quebra de vidro na orientação da Well-Architected AWS .

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem

ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços 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

Consulte Estrutura de adoção da AWS nuvem.

implantação canária

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

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

alterar captura de dados (CDC)

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

engenharia do caos

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

CI/CD

Veja a integração e a entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas 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 CCoEpostagens 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 geralmente está conectada à tecnologia de computação de ponta.

modelo operacional em nuvem

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

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam quando migram para o Nuvem AWS:

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

Esses estágios foram definidos por Stephen Orban na postagem do blog The Journey Toward Cloud-First & the Stages of Adoption no blog de estratégia Nuvem AWS empresarial. Para obter

informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

Um campo da IA que usa aprendizado de máquina para analisar e extrair informações de formatos visuais, como imagens e vídeos digitais. Por exemplo, AWS Panorama oferece dispositivos que adicionam CV às redes de câmeras locais, e a Amazon SageMaker fornece algoritmos de processamento de imagem para CV.

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

Um repositório que armazena e gerencia informações sobre um banco de dados e seu ambiente de TI, incluindo componentes de hardware e software e suas configurações. Normalmente, você usa dados de um CMDB 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 YAML modelo. 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. O CI/CD é comumente descrito como um pipeline. O CI/CD pode ajudar você a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte Benefícios da entrega contínua. CD também pode significar implantação contínua. Para obter mais informações, consulte Entrega contínua versus implantação contínua.

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

Um processo para identificar e categorizar os dados em sua rede com base em criticalidade e confidencialidade. É um componente crítico de qualquer estratégia de gerenciamento de riscos de segurança cibernética, pois ajuda a determinar os controles adequados de proteção e retenção para os dados. A classificação de dados é um componente do pilar de segurança no AWS Well-Architected Framework. Para obter mais informações, consulte Classificação de dados.

desvio de dados

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

dados em trânsito

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

malha de dados

Uma estrutura arquitetônica que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

Um sistema de gerenciamento de dados que oferece suporte à inteligência comercial, como análises. Os data warehouses geralmente contêm grandes quantidades de dados históricos e geralmente são usados para consultas e análises.

linguagem de definição de banco 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 banco de dados () DML

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

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta é chamada de administrador delegado para esse serviço Para obter mais informações e uma lista de serviços compatíveis, consulte Serviços que funcionam com o AWS Organizations na documentação do AWS Organizations .

implantação

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

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Consulte 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 você pode usar o design orientado por domínio com o padrão strangler fig, consulte Modernizando a Microsoft antiga. ASP NET(ASMX) serviços web incrementalmente usando contêineres e o Amazon API Gateway.

DR

Veja a recuperação de desastres.

detecção de deriva

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

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

computação de borda

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

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o endpoint do serviço.

serviço de endpoint

Um serviço que você pode hospedar em uma nuvem privada virtual (VPC) para compartilhar com outros usuários. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros Contas da AWS ou a AWS Identity and Access Management (IAM) principais. Essas contas ou diretores podem se conectar ao seu serviço de endpoint de forma privada criando endpoints de interface. VPC Para obter mais informações, consulte Criar um serviço de endpoint na documentação da Amazon Virtual Private Cloud (AmazonVPC).

planejamento de recursos corporativos (ERP)

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

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).

environment (ambiente)

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

- ambiente de desenvolvimento: uma instância de uma aplicação em execução que está disponível somente para a equipe principal responsável pela manutenção da aplicação. Ambientes de desenvolvimento são usados para testar mudanças antes de promovê-las para ambientes superiores. Esse tipo de ambiente às vezes é chamado de ambiente de teste.

- ambientes inferiores: todos os ambientes de desenvolvimento para uma aplicação, como aqueles usados para compilações e testes iniciais.
- ambiente de produção: uma instância de uma aplicação em execução que os usuários finais podem acessar. Em um pipeline de CI/CD, o ambiente de produção é o último ambiente de implantação.
- ambientes superiores: todos os ambientes que podem ser acessados por usuários que não sejam a equipe principal de desenvolvimento. Isso pode incluir um ambiente de produção, ambientes de pré-produção e ambientes para testes de aceitação do usuário.

epic

Em metodologias ágeis, categorias funcionais que ajudam a organizar e priorizar seu trabalho. Os epics fornecem uma descrição de alto nível dos requisitos e das tarefas de implementação. Por exemplo, os épicos de AWS CAF segurança 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

Consulte planejamento de recursos corporativos.

análise exploratória de dados () EDA

O processo de analisar um conjunto de dados para entender suas principais características. Você coleta ou agrega dados e, em seguida, realiza investigações iniciais para encontrar padrões, detectar anomalias e verificar suposições. EDAé realizado calculando estatísticas resumidas e criando visualizações de dados.

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a filial.

recursos

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

importância do recurso

O quanto um recurso é importante para as previsões de um modelo. Isso geralmente é expresso como uma pontuação numérica que pode ser calculada por meio de várias técnicas, como Shapley Additive Explanations () SHAP e gradientes integrados. Para obter mais informações, consulte Interpretabilidade do modelo de aprendizado de máquina com:AWS.

transformação de recursos

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

FGAC

Veja o controle de acesso refinado.

controle de acesso refinado () FGAC

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

migração flash-cut

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

G

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

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. Eles são implementados usando políticas de controle de serviços e limites de IAM permissões. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

migração homogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que compartilhe o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server RDS para Amazon for 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.

I

IaC

Veja a infraestrutura como código.

Política baseada em identidade

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

aplicação ociosa

Um aplicativo que tem uma média CPU de uso de 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 a Internet das Coisas industrial.

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que infraestruturas mutáveis. Para obter mais informações, consulte as melhores práticas de implantação usando infraestrutura imutável no Well-Architected AWS Framework.

entrada (entrada) VPC

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

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental

até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

inspeção VPC

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

Internet das Coisas (IoT)

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

interpretabilidade

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

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

Um conjunto de práticas recomendadas para fornecer serviços de TI e alinhar esses serviços a requisitos de negócios. ITILfornece a base paraITSM.

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 ITSM ferramentas, consulte o guia de integração de operações.

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiquetas () LBAC

Uma implementação do controle de acesso obrigatório (MAC) em que os usuários e os próprios dados 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.

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em rótulos.

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. 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.

ambientes inferiores

Veja o ambiente.

M

machine learning (ML)

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

ramificação principal

Veja a filial.

malware

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

serviços gerenciados

Serviços da AWS para o qual AWS opera a camada de infraestrutura, o sistema operacional e as plataformas, e você acessa os endpoints para armazenar e recuperar dados. O Amazon Simple

Storage Service (Amazon S3) e o Amazon DynamoDB são exemplos de serviços gerenciados. Eles também são conhecidos como serviços abstratos.

sistema de execução de manufatura (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

conta-membro

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

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens () MQTT

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

microsserviço

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

arquitetura de microsserviços

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

de uma interface bem definida usando leveza. APIs Cada microsserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte Implementação de microsserviços em. AWS

Programa de Aceleração de 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. MAPinclui 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 a Amazon EC2 com o AWS Application Migration Service.

Avaliação do portfólio de migração (MPA)

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

Avaliação da prontidão para migração () MRA

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

estratégia de migração

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

ML

Veja o aprendizado de máquina.

modernização

Transformar uma aplicação desatualizada (herdada ou monolítica) e sua infraestrutura em um sistema ágil, elástico e altamente disponível na nuvem para reduzir custos, ganhar eficiência e aproveitar as inovações. Para obter mais informações, consulte Estratégia para modernizar aplicativos no Nuvem AWS.

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte Avaliação da prontidão para modernização de aplicativos no. Nuvem AWS

aplicações monolíticas (monólitos)

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

MPA

Consulte Avaliação do portfólio de migração.

MQTT

Consulte Transporte de telemetria de enfileiramento de mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja o controle de acesso de origem.

OAI

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

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

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

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

OPC-EUA

Consulte Comunicação de processo aberto — Arquitetura unificada.

Comunicação de processo aberto - Arquitetura unificada (OPC-UA)

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

acordo de nível operacional () OLA

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

análise de prontidão operacional () ORR

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

tecnologia operacional (OT)

Sistemas de hardware e software que funcionam com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas OT e de tecnologia da informação (TI) é o foco principal das transformações da Indústria 4.0.

integração de operações (OI)

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

trilha organizacional

Uma trilha criada por ela AWS CloudTrail registra todos os eventos de 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.

gestão de mudanças organizacionais (OCM)

Uma estrutura para gerenciar grandes transformações de negócios disruptivas de uma perspectiva de pessoas, cultura e liderança. OCMajuda as organizações a se prepararem e fazerem a transição para novos sistemas e estratégias, acelerando a adoção de mudanças, 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 OCMguia.

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). OACoferece suporte a todos os buckets do S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e dinâmica `PUT` e `DELETE` solicitações ao bucket do S3.

identidade de acesso de origem (OAI)

Em CloudFront, uma opção para restringir o acesso para proteger seu conteúdo do Amazon S3. Quando você usaOAI, 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 controle de acesso mais granular e aprimorado.

ORR

Veja a análise de prontidão operacional.

NÃO

Veja a tecnologia operacional.

saída (saída) VPC

Em uma arquitetura de AWS várias contas, uma VPC que lida com 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 IAM de gerenciamento anexada aos IAM diretores para definir as permissões máximas que o usuário ou a função podem ter. Para obter mais informações, consulte Limites de permissões na IAM documentação.

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 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

Consulte controlador lógico programável.

PLM

Veja o gerenciamento do ciclo de vida do produto.

política

Um objeto que pode definir permissões (consulte a política baseada em identidade), especificar as condições de acesso (consulte a política baseada em recursos) ou definir as permissões máximas para todas as contas em uma organização em AWS Organizations (consulte a política de controle de serviços).

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pressão de predicados

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

controle preventivo

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

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma IAM função ou um usuário. Para obter mais informações, consulte os termos e conceitos do Diretor em Funções na IAM documentação.

Privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto () PLM

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

ambiente de produção

Veja o ambiente.

controlador lógico programável () PLC

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

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.

publicar/assinar (pub/sub)

Um padrão que permite comunicações assíncronas entre microsserviços para melhorar a escalabilidade e a capacidade de resposta. Por exemplo, em um microsserviço baseado em microsserviços MES, um microsserviço pode publicar mensagens de eventos em um canal no qual outros microsserviços possam se inscrever. O sistema pode adicionar novos microsserviços sem alterar o serviço de publicação.

Q

plano de consulta

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

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

RACImatriz

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

ransomware

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

RASCImatriz

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

RCAC

Veja o controle de acesso por linha e coluna.

réplica de leitura

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

rearquiteta

Veja 7 Rs.

objetivo do ponto de recuperação (RPO)

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

Região

Uma coleção de AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter mais informações, consulte Especificar o que Regiões da AWS sua conta pode usar.

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, responsável, 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 RASCImatriz e, se você excluí-la, ela será chamada de RACImatriz.

controle responsivo

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

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

rotação

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

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

S

SAML2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login AWS Management Console ou chamar as AWS API operações sem que você precise criar um usuário IAM para todos em sua organização. Para obter mais informações sobre a federação SAML baseada em 2.0, consulte Sobre a federação SAML baseada em 2.0 na documentação. IAM

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele consiste no valor secreto e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte O que há em um segredo do Secrets Manager? na documentação do Secrets Manager.

controle de segurança

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

fortalecimento da segurança

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

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

Ferramentas e serviços que combinam sistemas de gerenciamento de informações de segurança (SIM) e gerenciamento de eventos de segurança (SEM). Um SIEM sistema 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 VPC de segurança, a correção de uma EC2 instância da Amazon ou a rotação de credenciais.

Criptografia do lado do servidor

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

política de controle de serviço (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização no AWS Organizations. SCPsdefina 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.

contrato de nível de serviço () SLA

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

indicador de nível de serviço () SLI

Uma medida de um aspecto de desempenho de um serviço, como taxa de erro, disponibilidade ou taxa de transferência.

objetivo de nível de serviço () SLO

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

modelo de responsabilidade compartilhada

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

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

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

SLA

Veja o contrato de nível de serviço.

SLI

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte Abordagem em fases para modernizar aplicativos no. Nuvem AWS

SPOF

Veja um único ponto de falha.

esquema de estrelas

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

padrão strangler fig

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

sub-rede

Uma variedade de endereços IP em seuVPC. Cada sub-rede fica alocada em uma única zona de disponibilidade.

controle de supervisão e aquisição de dados () SCADA

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas de gerenciamento para você. Para obter mais informações, consulte Usando AWS Organizations com outros AWS serviços na AWS Organizations documentação.

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o ambiente.

V

aspiração

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

controle de versões

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

VPCespiando

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

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

workload

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

workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

WORM

Veja escrever uma vez, ler muitas.

WQF

Consulte Estrutura de qualificação AWS da carga de trabalho.

escreva uma vez, leia muitos (WORM)

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

Z

exploração de dia zero

Um ataque, geralmente malware, que tira proveito de uma vulnerabilidade de dia zero.

vulnerabilidade de dia zero

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

aplicação zumbi

Um aplicativo que tem uma média CPU e um uso de memória abaixo de 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.