Gerenciando identidade e acesso para o VMware Cloud on AWS

AWS Orientação prescritiva

AWS Orientação prescritiva: Gerenciando identidade e acesso para o VMware Cloud on AWS

Table of Contents

Gerenciar identidade e acesso ao VMware Cloud na AWS

Richard Milner-Watts, Abdenour Kansab e Chris Porter, Amazon Web Services (AWS)

Vern Bolinius, VMware

Junho de 2023 (histórico do documento)

Gerenciamento de identidade e acesso é o princípio de limitar o acesso aos sistemas somente a usuários e aplicações autorizados, incluindo restringir o acesso somente aos recursos de rede necessários. Em ambientes de nuvem, os controles de gerenciamento de identidade e acesso geralmente consistem nas políticas e serviços que você usa para identificar, autenticar e autorizar usuários, grupos de usuários e aplicações.

O VMware Cloud na AWS oferece suporte a workloads baseadas no VMware vSphere na Nuvem AWS. É possível usar vários serviços e ferramentas da VMware para configurar, gerenciar, fazer backup, monitorar e analisar essa infraestrutura de nuvem. Os recursos e controles que você usa para gerenciar a identidade e o acesso variam entre os serviços. Este documento fornece práticas recomendadas e outras recomendações para gerenciar a identidade e o acesso aos seguintes serviços da VMware:

- VMware Aria Operations
- Operações do VMware Aria for Logs
- VMware Aria Operations for Networks
- VMware Cloud Disaster Recovery
- VMware Cloud na AWS
- VMware Cloud Services Console
- VMware HCX
- VMware NSX
- VMware Site Recovery
- VMware vCenter Server

Este guia fornece uma visão geral e apresenta práticas recomendadas de gerenciamento de identidade e acesso para o VMware Cloud na AWS e serviços relacionados da VMware. Ele inclui uma breve descrição de cada serviço e discute as considerações de gerenciamento de identidade e

acesso desse serviço. Também fornecemos recomendações para configurar o serviço como parte do VMware Cloud na AWS.

> **Important**
>
> Muitos dos serviços da VMware discutidos neste guia são usados em outras soluções da VMware na nuvem ou on-premises. As recomendações e as práticas recomendadas deste guia são específicas para o VMware Cloud na AWS. Essas recomendações podem não se aplicar a outros ambientes.

Público-alvo

Este guia é voltado para arquitetos e engenheiros de segurança responsáveis pela implementação do VMware Cloud na AWS em ambientes de nuvem ou híbridos.

Resultados de negócios desejados

Este guia ajuda você a:

1. Entender os vários controles de gerenciamento de identidade e acesso do VMware Cloud na AWS e serviços relacionados da VMware
2. Familiarizar-se com as práticas recomendadas que ajudam você a operar com segurança o VMware Cloud na AWS
3. Entenda as opções disponíveis para autenticação federada por meio de um provedor de identidade externo

Visão geral do gerenciamento de identidades

A VMware usa os seguintes conceitos e hierarquia de identidade padrão do setor para gerenciar a identificação, a autenticação e a autorização:

- Usuários são as pessoas que acessam seu ambiente de alguma forma. É possível criar usuários locais ou usar a federação para autenticar usuários de um provedor de identidade externo. Para obter mais informações, consulte Federação de identidade e SSO.
- Grupos fornecem um mecanismo para agrupar logicamente uma coleção de usuários. Isso ajuda você a conceder permissões consistentes a esses usuários e reduz a sobrecarga administrativa. Os perfis são usados para conceder permissões a um usuário ou grupo. Para obter mais informações, consulte Perfis e permissões no SDDC (documentação da VMware).
- Organizations no VMware Cloud controlam o acesso a um ou mais serviços da VMware. Os usuários e grupos devem pertencer a uma organização para acessar os serviços na organização. É possível habilitar o recurso de Governança e administração de identidades para permitir que identidades federadas solicitem, por autoatendimento, a associação a uma organização da VMware. Para obter mais informações, consulte VMware Cloud Services Console.

As permissões podem conceder acesso a um objeto específico ou podem ser herdadas dos objetos pais. Se várias permissões sobrepostas forem atribuídas a um usuário ou grupo, a permissão mais permissiva será aplicada. Para obter mais informações, consulte Herança hierárquica de permissões (documentação da VMware).

Você pode usar esses elementos estruturais para adotar uma política de privilégios mínimos e estabelecer limites lógicos de acesso em sua infraestrutura com base nos requisitos do usuário. Privilégio mínimo é o princípio de conceder aos usuários e aplicações somente o acesso mínimo necessário para realizar suas tarefas. No caso de acesso não autorizado, essa prática recomendada do setor pode ajudar a limitar a capacidade do invasor de causar danos ou roubar dados confidenciais. E mesmo para usuários autorizados, esse princípio pode impedir que os usuários acessem dados que não deveriam. Oferecer aos usuários acesso somente aos recursos necessários também pode melhorar a produtividade e reduzir a necessidade de suporte para solução de problemas.

Ao usar o VMware Cloud na AWS, há dois serviços e ferramentas principais para gerenciar identidade e acesso: VMware Cloud Services Console e VMware vCenter Server. Posteriormente neste guia, discutiremos esses serviços com mais detalhes.

Federação de identidade e SSO

Muitas empresas querem configurar uma federação com um provedor de identidades (IdP) externo. Isso permite a você fornecer uma experiência de autenticação única (SSO) para seus usuários. Tanto o VMware Cloud quanto o vCenter Server oferecem suporte à federação corporativa:

- O VMware Cloud oferece suporte a IDPs baseados em Security Assertion Markup Language (SAML) 2.0 e ao Lightweight Directory Access Protocol (LDAP). Para obter mais informações, consulte O que é federação corporativa e como ela funciona com os VMware Cloud Services (documentação da VMware).
- Quando o vCenter Server é executado no VMware Cloud na AWS, não há suporte à federação com o vCenter Server usando um IdP externo. Somente o IdP integrado pode ser usado, o qual permite usar o Microsoft Active Directory via LDAP. Para obter mais informações, consulte Fontes de identidade para vCenter Server com vCenter Single Sign-On (documentação da VMware).

Alguns dos outros serviços da VMware relacionados discutidos neste guia também oferecem suporte à federação direta a partir de um IdP. No entanto, configurar a federação em cada serviço cria pontos adicionais de gerenciamento de usuários e se torna difícil de gerenciar. Em vez disso, é possível usar grupos e perfis no VMware Cloud Services Console para usar uma fonte de identidade comum e configurar permissões para outros serviços do VMware Cloud. Além disso, você pode configurar o Modo vinculado híbrido para usar as mesmas identidades com uma instância on-premises do vCenter Server. Isso reduz o número de pontos de federação e gerenciamento de identidade para dois serviços. Para obter mais informações sobre o Modo vinculado híbrido, consulte Configurar o Modo vinculado híbrido (documentação da VMware).

Práticas recomendadas gerais

> **Important**
>
> Muitos dos serviços da VMware discutidos neste guia são usados em outras soluções da VMware na nuvem ou on-premises. As recomendações e as práticas recomendadas deste guia são específicas para o VMware Cloud na AWS. Essas recomendações podem não se aplicar a outros ambientes.

Considere as seguintes recomendações da AWS para gerenciar a identidade e o acesso à sua infraestrutura de nuvem da VMware:

- Aplique uma política de privilégio mínimo. Use o controle de acesso baseado em perfil (RBAC) para conceder o acesso e as permissões mínimas necessárias para que os usuários desempenhem suas funções.
- Quando possível, conceda permissões a grupos em vez de a usuários individuais.
- Evite configurar usuários locais. Autentique usuários em um provedor de identidade federado externo.
- Configure a autenticação multifator para todos os usuários.
- Sua política de senhas deve incluir requisitos de força e alternância de senhas.
- Documente um procedimento de quebrar o vidro para assumir o controle administrativo total sobre a organização da VMware e os serviços relacionados. “Quebrar o vidro”, cujo nome vem de quebrar o vidro para acionar um alarme de incêndio, refere-se a um meio de uma pessoa obter rapidamente acesso administrativo em circunstâncias excepcionais usando um processo aprovado e auditado.
- Se você tiver data centers on-premises ou várias instâncias do vCenter Server, use o Modo vinculado híbrido para conectar sua instância do vCenter Server na nuvem ao domínio do vCenter Single Sign-On. Isso ajuda a gerenciar seus recursos on-premises e na nuvem a partir de uma única interface do vSphere Client.
- Quando possível, configure os endpoints de gerenciamento, como o vCenter Server, o HCX Cloud Manager e o NSX Manager, para que possam ser acessados somente por redes internas, e não pela Internet pública.
- Não use credenciais locais, como a conta cloudadmin, para fins administrativos. Reserve essas contas para uso em seu procedimento de quebra de vidro. As ações realizadas usando contas

de usuário administrativas locais não podem ser atribuídas a um indivíduo específico e, portanto, essas contas poderiam ser usadas para fazer alterações sem responsabilidade.

- Altere as senhas da conta de usuário locais, como os usuários raiz e administrativos, para valores fortes e armazene com segurança essas credenciais em um armazenamento de senhas auditado. Estabeleça um processo de aprovação para conceder acesso a essas senhas.
- Se as credenciais locais persistirem por longos períodos, como por vários meses ou mais, estabeleça um processo para alternar as credenciais (por exemplo, se você estiver usando o VMware HCX para ampliar uma rede).

Essas recomendações se aplicam a todas as configurações de serviço da VMware para o VMware Cloud na AWS. Recomendações adicionais para cada serviço são abordadas posteriormente neste guia.

Serviços de gerenciamento de identidade da VMware

Ao usar o VMware Cloud na AWS, há dois serviços e ferramentas principais para gerenciar identidade e acesso: VMware Cloud Services Console e VMware vCenter Server.

VMware Cloud Services Console

O VMware Cloud Services Console (documentação da VMware) ajuda você a gerenciar seu portfólio de serviços do VMware Cloud, inclusive o VMware Cloud na AWS. Nesse serviço, você pode:

- Gerenciar entidades, como usuários e grupos
- Gerenciar organizações que controlam o acesso a outros serviços de nuvem, como o VMware Cloud Disaster Recovery (VCDR) e o VMware Aria Suite
- Atribuir perfis a recursos e serviços
- Visualizar as aplicações OAuth que têm acesso à sua organização
- Configurar a federação corporativa para a organização
- Habilitar e implantar serviços do VMware Cloud, como o VMware Aria e o VMware Cloud na AWS
- Gerenciar cobranças e assinaturas
- Obter suporte da VMware

Gerenciar identidades e acessos

Ao configurar adequadamente usuários, grupos, perfis e organizações no VMware Cloud Services Console, é possível implementar uma política de acesso com privilégio mínimo.

Proteger o acesso ao VMware Cloud Services Console é fundamental porque os usuários administrativos desse serviço podem alterar as permissões em todo o ambiente de nuvem da VMware e acessar informações confidenciais, como informações de cobrança. Para acessar todos os recursos do console, como cobrança e suporte, os usuários também devem estar vinculados a um perfil do VMware Customer Connect (formalmente conhecido como MyVMware).

No VMware Cloud Services Console, use os seguintes tipos de perfis para conceder permissões a usuários e grupos:

- Perfis da organização: esses perfis se referem diretamente à organização do VMware Cloud, concedendo permissões no VMware Cloud Services Console. Há duas perfis padrão. Proprietário

da organização: perfil com permissão total para administrar a organização. Membro da organização: perfil com acesso de leitura ao VMware Cloud Services Console. Para obter mais informações, consulte Que perfis organizacionais estão disponíveis no VMware Cloud Services Console (documentação da VMware).

- Perfis de serviço: esses perfis permitem que você atribua permissões para usar um serviço específico. Por exemplo, uma entidade com o perfil de serviço DR Admin pode administrar o VMware Cloud Disaster Recovery (VCDR) no console de serviço dedicado. Cada serviço disponível na organização tem uma ou mais perfis de serviço associados. Para obter mais informações sobre os perfis de serviço disponíveis, consulte a documentação da VMware para o serviço de interesse.

O VMware Cloud Services Console oferece suporte a políticas de autenticação. Eles podem estipular que um usuário deve fornecer um segundo token de autenticação ao fazer login, também conhecido como autenticação multifator (MFA).

Para obter mais informações sobre o gerenciamento de identidade e acesso nesse serviço, consulte Gerenciamento de identidade e acesso (documentação da VMware).

Recomendações da AWS

Além das Práticas recomendadas gerais, a AWS recomenda o seguinte ao configurar o VMware Cloud Services Console para VMware Cloud na AWS:

- Ao criar uma organização, use um perfil do VMware Customer Connect e um endereço de e-mail corporativo associado que não pertença a um indivíduo, como vmwarecloudroot@example.com. Essa conta deve ser tratada como uma conta de serviço ou raiz, e você deve auditar o uso e restringir o acesso à conta de e-mail. Configure imediatamente a federação de contas com seu provedor de identidades (IdP) corporativo para que os usuários possam acessar a organização sem usar essa conta. Reserve essa conta para uso em um procedimento de quebra de vidro para resolver problemas com o IdP federado.
- Use identidades federadas para que a organização conceda acesso a outros serviços de nuvem, como o VMware Cloud Disaster Recovery (VCDR). Não gerencie individualmente usuários ou federações em serviços diferentes. Isso simplifica o gerenciamento do acesso a vários serviços, como quando os usuários entram ou saem da empresa.
- Atribua o perfil de Proprietário da organização com moderação. As entidades com esse perfil podem conceder a si mesmas acesso total a todos os aspectos da organização e a quaisquer serviços de nuvem associados.

VMware vCenter Server

O VMware vCenter Server (site da VMware) é um plano de gerenciamento para administrar ambientes do VMware vSphere. No vCenter Server, gerencie as entidades que podem acessar os recursos do vSphere, como máquinas virtuais, e acessar complementos, como o VMware HCX e o VMware Site Recovery. Gerencie o vCenter Server por meio da aplicação vSphere Client. O vCenter Server permite:

- Gerenciar máquinas virtuais, hosts VMware ESXi e armazenamento do VMware vSAN
- Configurar e gerenciar o vCenter Single Sign-On

Se você tiver data centers on-premises, poderá usar o modo vinculado híbrido para vincular sua instância do vCenter Server na nuvem a um domínio do vCenter Single Sign-On on-premises. Se o domínio do vCenter Single Sign-On contiver várias instâncias do vCenter Server conectadas usando o Modo vinculado avançado, todas essas instâncias serão vinculadas ao seu SDDC na nuvem. Ao usar esse modo, você pode visualizar e gerenciar seus data centers on-premises e na nuvem a partir de uma única interface do vSphere Client e migrar workloads entre seu data center on-premises e o SDDC na nuvem. Para obter mais informações, consulte Configurar o Modo vinculado híbrido (documentação da VMware).

Gerenciar identidades e acessos

Em datacenters definidos por software (SDDCs) (site da VMware) para o VMware Cloud na AWS, a forma de operar o vCenter Server é semelhante à de um SDDC on-premises. A principal diferença é que o VMware Cloud na AWS é um serviço gerenciado. Portanto, a VMware é responsável por determinadas tarefas administrativas, como gerenciamento de hosts, clusters e gerenciamento de máquinas virtuais. Para obter mais informações, consulte O que há de diferente na nuvem? e Permissões globais (documentação da VMware).

Como a VMware executa algumas tarefas administrativas para o SDDC, um administrador de nuvem exige menos privilégios do que um administrador de um data center on-premises. Quando você cria um SDDC do VMware Cloud na AWS, um usuário cloudadmin é criado automaticamente e recebe o perfil CloudAdmin (documentação da VMware). Essa conta de usuário local privilegiada pode ser usada para acessar o vCenter Server e o vCenter Single Sign-On. Usuários que tem o perfil de serviço Administrador ou Administrador (restrição de exclusão) do VMware Cloud na AWS no VMware Cloud Services Console podem obter as credenciais para o usuário cloudadmin. O perfil CloudAdmin tem o máximo de permissões possíveis no vCenter Server para um SDDC do VMware

Cloud na AWS. Para obter mais informações sobre este perfil de serviço, consulte Privilégios do CloudAdmin(documentação da VMware). O usuário cloudadmin é o único usuário local disponível para o vCenter Server no VMware Cloud na AWS. Para conceder acesso a outros usuários, use uma fonte de identidade externa.

O vCenter Single Sign-On é um agente de autenticação que fornece infraestrutura de troca de tokens de segurança. Quando um usuário se autentica no vCenter Single Sign-On, recebe um token que ele pode usar para se autenticar no vCenter Server e outros serviços complementares usando chamadas a API. O usuário cloudadmin pode configurar uma fonte de identidade externa para o vCenter Server. Para obter mais informações, consulte Fontes de identidade para vCenter Server com vCenter Single Sign-On (documentação da VMware).

No VMware Cloud Services Console, use três tipos de perfis para conceder permissões a usuários e grupos:

- Perfis do sistema: não é possível editar ou excluir esses perfis.
- Perfis de exemplo: esses perfis representam combinações de tarefas executadas com frequência. É possível copiar, editar ou excluir esses perfis.
- Perfis personalizados: se o sistema e os perfis de exemplo não fornecerem o controle de acesso desejado, você poderá criar funções personalizadas no vSphere Client. É possível duplicar e modificar um perfil existente ou criar um novo perfil. Para obter mais informações, consulte Criar um perfil personalizado do vCenter Server(documentação da VMware).

Para cada objeto no inventário do SDDC, é possível atribuir somente um perfil a um usuário ou grupo. Se, para um único objeto, um usuário ou grupo exigir uma combinação de perfis integrados, há duas opções. A primeira opção é criar um perfil personalizado com as permissões necessárias. A outra opção é criar dois grupos, atribuir um perfil interno a cada um e, em seguida, adicionar o usuário aos dois grupos.

Recomendações da AWS

Além das Práticas recomendadas gerais, a AWS recomenda o seguinte ao configurar o vCenter Server para VMware Cloud na AWS:

- Use a conta de usuário cloudadmin para configurar uma fonte de identidade externa no vCenter Single Sign-On. Atribua usuários apropriados da fonte de identidade externa para serem usados para fins administrativos e, em seguida, interrompa o uso do usuário cloudadmin. Para ver as

práticas recomendadas ao configurar o vCenter Single Sign-On, consulte Segurança e acesso às informações para o vCenter Server (documentação da VMware).

- No vSphere Client, atualize as credenciais cloudadmin para cada instância do vCenter Server para um novo valor e, em seguida, armazene-as em segurança. Essa alteração não se reflete no VMware Cloud Services Console. Por exemplo, a visualização das credenciais por meio do Cloud Services Console mostra o valor original.

> **Note**
>
> Se as credenciais dessa conta forem perdidas, o suporte da VMware poderá redefini-las.

- Não use a conta cloudadmin para realizar as tarefas do dia a dia. Reserve essa conta para uso como parte de um procedimento de quebra de vidros.
- Restrinja o acesso ao vCenter Server somente por meio de redes privadas.

Serviços relacionados a VMware

Este capítulo fornece práticas recomendadas e outras recomendações para gerenciar a identidade e o acesso aos seguintes serviços da VMware relacionados ao VMware Cloud na AWS:

- Serviços gerenciados por meio do VMware Cloud Services Console:
  - VMware Cloud na AWS
  - VMware NSX
  - Operações do VMware Aria for Logs
  - VMware Aria Operations for Networks
  - VMware Aria Operations
  - VMware Cloud Disaster Recovery
- Serviços gerenciados por meio do VMware vCenter Server:
  - VMware HCX
  - VMware Site Recovery

Este guia fornece uma breve descrição de cada serviço, discute os controles de identidade e gerenciamento de acesso para o serviço e inclui recomendações da AWS para configurar esse serviço como parte do VMware Cloud na AWS.

VMware Cloud na AWS

O VMware Cloud na AWS (documentação da VMware) é um serviço desenvolvido em conjunto pela AWS e a VMware para ajudar você a migrar e estender seus ambientes on-premises baseados no VMware vSphere para a Nuvem AWS.

Se você pertencer a uma organização que concede acesso a esse serviço, poderá acessar o VMware Cloud na AWS por meio do VMware Cloud Services Console. O VMware Cloud na AWS permite:

- Criar e excluir SDDCs.
- Administrar grupos de SDDCs.
- Administrar SDDCs, incluindo parâmetros de rede e cluster.

- Acessar as credenciais do usuário cloudadmin do VMware vCenter Server. Para obter mais informações sobre este usuário, consulte VMware vCenter Server neste guia.
- Acessar as credenciais do usuário cloud_admin do VMware NSX. Para obter mais informações sobre este usuário, consulte VMware NSX neste guia.
- Ativar e implantar serviços complementares em SDDCs, como o VMware Site Recovery e o VMware HCX.
- Acessar consoles para serviços complementares, incluindo HCX e VMware Site Recovery.

Gerenciar identidades e acessos

Use o VMware Cloud Services Console para gerenciar identidades e acesso ao VMware Cloud na AWS. Para o VMware Cloud na AWS, os seguintes perfis de serviço estão disponíveis:

- Administrador: perfil que oferece acesso total ao VMware Cloud na AWS.
- Administrador (restrição de exclusão): perfil que oferece acesso total ao VMware Cloud na AWS, exceto as operações de exclusão de SDDCs.
- Administrador do NSX Cloud
- Auditor do NSX Cloud

> **Note**
>
> Os perfis Administrador do NSX Cloud e Auditor do NSX estão relacionados ao uso do VMware NSX. Para obter mais informações, consulte VMware NSX.

Um dos dois perfis de Administrador é necessário para acessar um SDDC no Cloud Services Portal. Usuários sem nenhum dos dois perfis do NSX Cloud não podem acessar a guia Rede e segurança do SDDC no Cloud Services Portal. Além disso, eles não podem acessar as credenciais de administrador do NSX.

Recomendações da AWS

Além das Práticas recomendadas gerais, a AWS recomenda o seguinte ao configurar o VMware Cloud na AWS:

- Para conceder acesso aos administradores, use somente o perfil Administrador (restrição de exclusão). Reserve o perfil Administrador para acesso rápido de emergência quando precisar excluir um SDDC.
- Não conceda os perfis do NSX a usuários que não precisam acessar as configurações de rede e firewall. Para obter mais informações, consulte VMware NSX neste guia.
- Altere as senhas da conta de usuário local cloudadmin para um valor forte e armazene com segurança essas credenciais em um armazenamento de senhas auditado. É possível alterar essa senha no VMware vCenter Server com o vSphere Web Client.

VMware NSX

O VMware NSX (documentação da VMware) fornece uma camada de virtualização de rede que reproduz o modelo de interconexão de sistemas abertos (OSI) da camada 2 à camada 7 e inclui recursos como comutação, roteamento e firewalls. Há duas versões do NSX. A versão original (NSX-V) exige que o vCenter Server também seja implantado. A versão mais recente (NSX-T) é desacoplada do vCenter Server, o que possibilita o suporte a arquiteturas híbridas. O VMware Cloud na AWS usa o NSX-T.

O NSX, junto com o vSphere e o vSAN, é um componente essencial do VMware Cloud na AWS. O NSX fornece toda a funcionalidade de rede em um SDDC e gerencia a interação entre a rede de sobreposição e os componentes nativos da AWS que formam a base da rede. O NSX é fortemente acoplado a outros serviços, como o vCenter Server e o VMware HCX, os quais chamam as APIs do NSX para gerenciar recursos.

O NSX permite:

- Gerenciar a comutação e o roteamento
- Gerenciar firewalls, inclusive usando um firewall distribuído para inspeção em linha entre VMs ou entre a rede e a Internet pública
- Gerenciar redes privadas virtuais (VPNs)
- Configurar o Protocolo de Configuração Dinâmica de Host (DHCP) e o Sistema de Nomes de Domínio (DNS)

É possível acessar o NSX via VMware Cloud Services Console ou por meio da interface de usuário Web (IU) dedicada do NSX Manager. A interface Web do NSX Manager oferece alguns recursos adicionais que não estão disponíveis no VMware Cloud Services Console. Para obter mais

informações, consulte Administração de rede de SDDCs com o NSX Manager(documentação da VMware).

Observe o seguinte ao acessar o NSX no VMware Cloud na AWS:

- Para acessar o NSX por meio do VMware Cloud Services Console, você deverá ter o perfil Administrador do VMware Cloud na AWS atribuído. Você pode acessar o NSX na guia Rede e segurança do SDDC. Para obter mais informações sobre este perfil, consulte VMware Cloud na AWS neste guia.
- É possível abrir a interface do usuário Web do NSX Manager escolhendo o link na guia Configurações do SDDC ou escolhendo Abrir o NSX Manager na página Resumo do SDDC. Para obter mais informações, consulte Abrir o NSX Manager (documentação da VMware).
- Se o SDDC estiver no modo Payment Card Industry Data Security Standard (PCI DSS), não será possível acessar o NSX por meio da guia Rede e segurança do VMware Cloud Services Console. Você deve usar a interface do usuário Web do NSX Manager.

Gerenciar identidades e acessos

Use o VMware Cloud Services Console para gerenciar identidades e acesso ao VMware NSX. Para o NSX no VMware Cloud na AWS, os seguintes perfis de serviço estão disponíveis:

- Administrador do NSX Cloud: permite administrar a funcionalidade do VMware NSX com o VMware Cloud na AWS.
- Auditor do NSX Cloud: esse perfil pode visualizar as configurações e os eventos do serviço NSX, mas não pode fazer nenhuma alteração.

> **Note**
>
> Apesar dos nomes, esses perfis não estão relacionados ao serviço VMware NSX Cloud.

Os seguintes usuários podem acessar o NSX:

- O usuário local cloud_admin, que é um usuário NSX local integrado e altamente privilegiado. Usuários com o perfil Administrador do NSX Cloud podem acessar as credenciais dessa conta de usuário. Apesar de seus nomes semelhantes, o usuário cloud_admin é diferente do usuário local cloudadmin@vmc.local do vCenter Single Sign-On.

- Usuários aos quais o perfil de serviço Administrador do NSX Cloud ou o perfil de serviço Auditor do NSX Cloud no VMware Cloud Services Console foi atribuído. Esses usuários podem ser usuários do VMware Cloud Services Console ou usuários federados externamente.
- Usuários que receberam acesso direto ao NSX por uma fonte de identidade via LDAP.

Recomendações da AWS

Além das Práticas recomendadas gerais, a AWS recomenda o seguinte ao configurar o NSX para VMware Cloud na AWS:

- Se sua empresa tiver usuários responsáveis pelo gerenciamento de redes e firewalls, mas não pelo gerenciamento de SDDCs, conceda a esses usuários um dos perfis do NSX, mas o perfil de Administrador. Esses usuários devem acessar o NSX por meio da interface do usuário Web do NSX Manager.
- Altere as senhas da conta de usuário local cloud_admin para um valor forte e armazene com segurança essas credenciais em um armazenamento de senhas auditado. Para alterar essa senha, é necessário entrar em contato com o suporte da VMware.
- Evite conceder acesso a usuários externos diretamente no NSX. Em vez disso, configure a federação corporativa no VMware Cloud Services Console e use perfis e grupos para conceder acesso a esse serviço.

Operações do VMware Aria for Logs

O VMware Aria Operations for Logs (documentação da VMware), antigo VMware vRealize Log Insight Cloud, é uma ferramenta de armazenamento e análise de logs que ajuda você a visualizar e consultar os dados de logs produzidos por seus SDDCs da VMware. O VMware Aria Operations for Logs permite:

- Realizar a integração com instâncias on-premises do vRealize Operations
- Coletar e analisar todos os tipos de dados de logs gerados por máquinas
- Configurar alertas
- Monitorar e analisar logs de outros serviços da VMware

Há duas versões desse serviço centralizado de gerenciamento de logs. O VMware vRealize Log Insight é uma versão on-premises que pode ser executada como um dispositivo em seu SDDC.

O VMware Aria Operations for Logs é uma versão no formato software como serviço (SaaS). O VMware Cloud na AWS usa a versão em nuvem como o serviço de log padrão, e isso não pode ser alterado. Se você usa a versão on-premises, é necessário encaminhar os logs da instância na nuvem para sua instância on-premises.

O VMware Aria Operations for Logs está incluído no VMware Cloud na AWS. A versão incluída oferece capacidade de ingestão e período de retenção de armazenamento limitados. Se necessário, você faça o upgrade para uma assinatura premium para aumentar esses limites. Para obter mais informações, consulte Assinaturas e cobrança (documentação da VMware).

Gerenciar identidades e acessos

Use o VMware Cloud Services Console para gerenciar identidades e acesso ao VMware Aria Operations for Logs. O VMware Aria Operations for Logs usa os mesmos usuários, incluindo identidades federadas e grupos, configurados no VMware Cloud Services Console. Para conceder permissões para esse serviço, é possível atribuir um perfil de serviço ou configurar um perfil personalizado no VMware Aria Operations for Logs. Para obter mais informações, consulte Perfis de serviço (documentação da VMware).

O VMware vRealize Log Insight tem dois perfis padrão. O perfil de Administrador tem acesso e controle totais, enquanto o perfil de Usuário tem acesso de leitura e pode criar painéis. É possível usar perfis personalizados para conceder acesso somente a conjuntos de dados específicos. Esses conjuntos de dados contêm filtros que restringem quais dados de log estão disponíveis para o usuário. Para obter mais informações, consulte Criar um conjunto de dados (documentação da VMware).

Recomendações da AWS

Siga as Práticas recomendadas gerais descritas anteriormente neste guia. Não temos recomendações adicionais para gerenciar identidades e acesso neste serviço.

VMware Aria Operations for Networks

O VMware Aria Operations for Networks, antigo VMware vRealize Network Insight Cloud, é uma versão SaaS do vRealize Network Insight. O VMware vRealize Network Insight (documentação da VMware) ajuda você a entender os fluxos de tráfego para suas workloads. Esse serviço pode ser usado para diagnosticar problemas de rede e modelar regras de firewall para oferecer suporte à segmentação de workloads. O VMware Aria Operations for Networks permite:

- Visualizar seus ambientes híbridos e multinuvem
- Solucionar problemas e analisar fluxos de tráfego
- Detectar e analisar aplicações
- Mapear dependências entre workloads

Existem três versões desse serviço. O VMware vRealize Network Insight é uma versão somente para uso on-premises. O VMware Aria Operations for Networks é uma versão SaaS. O vRealize Network Insight Universal pode ser implantado como uma solução on-premises ou como uma solução SaaS de nuvem federada. Todas as versões são compatíveis com o VMware Cloud na AWS.

Gerenciar identidades e acessos

Use o VMware Cloud Services Console para gerenciar identidades e acesso ao VMware Aria Operations for Networks. O VMware Aria Operations for Networks usa os mesmos usuários, incluindo identidades federadas e grupos, configurados no VMware Cloud Services Console. Para o VMware Aria Operations for Networks, os seguintes perfis de serviço estão disponíveis:

- Administrador: perfil com acesso e controle totais.
- Membro: perfil com acesso limitado.
- Auditor: perfil com acesso somente leitura.

Recomendações da AWS

Siga as Práticas recomendadas gerais descritas anteriormente neste guia. Não temos recomendações adicionais para gerenciar identidades e acesso neste serviço.

VMware Aria Operations

O VMware Aria Operations (documentação da VMware), antigo VMware vRealize Operations Cloud, é uma plataforma de gerenciamento de operações para VMware Cloud na AWS. Esse serviço usa inteligência artificial e machine learning (IA/ML) para ajudar você a otimizar, planejar e escalar as aplicações e a infraestrutura em suas implantações de nuvem híbrida. O VMware Aria Operations permite:

- Visualizar recomendações de otimização baseadas em IA/ML para performance e capacidade

- Gerenciar configurações de conformidade e recursos
- Acessar ferramentas para ajudar a solucionar problemas, por exemplo, resolver problemas de clientes ou responder a alertas
- Use pacotes de gerenciamento (documentação da VMware) para expandir os recursos de monitoramento, solução de problemas e remediação desse serviço

Há duas versões desse serviço de gerenciamento de operações. O VMware vRealize Operations é uma versão on-premises que pode ser executada como um dispositivo em seu SDDC. O VMware Aria Operations é uma versão no formato software como serviço (SaaS) do vRealize Operations. Ambas as versões são compatíveis com o VMware Cloud na AWS. Como o VMware Cloud na AWS é um serviço gerenciado e o acesso a alguns recursos é restrito, nem todos os recursos do vRealize Operations são compatíveis. Para obter mais informações, consulte Limitações conhecidas (documentação da VMware).

Gerenciar identidades e acessos

Use o VMware Cloud Services Console para gerenciar identidades e acesso ao VMware Aria Operations. O VMware Aria Operations usa os mesmos usuários, incluindo identidades federadas, configurados no VMware Cloud Services Console. Para conceder permissões para esse serviço, é possível atribuir um perfil de serviço ou configurar um perfil personalizado no VMware Aria Operations. Para obter mais informações sobre os perfis de serviço disponíveis, consulte Perfis e privilégios(documentação da VMware).

Há três perfis integrados: Administrador, Usuário geral e Somente leitura e, se necessário, é possível criar perfis personalizados para atender a requisitos de permissões específicos. É possível criar grupos para minimizar a sobrecarga administrativa do gerenciamento de permissões para vários usuários.

A versão on-premises do VMware vRealize Operations oferece suporte a usuários locais, enquanto as versões na nuvem e on-premises oferecem suporte a usuários federados. No entanto, a federação de usuários com um provedor de identidade externo varia entre as versões on-premises e na nuvem do vRealize Operations. Na versão on-premises, é possível federar diretamente os usuários de um IdP externo via LDAP ou usar as identidades federadas no vCenter Server. Na versão em nuvem, use os mesmos usuários, incluindo usuários federados, configurados por você no VMware Cloud Services Console.

Recomendações da AWS

Além das Práticas recomendadas gerais, a AWS recomenda o seguinte ao configurar o VMware Aria Operations para VMware Cloud na AWS:

- Evite federar usuários diretamente. Para a versão em nuvem, federe os usuários no VMware Cloud Services Console e, em seguida, use perfis e grupos para conceder acesso a esse serviço. Para a versão on-premises desse serviço, use identidades de uma fonte autenticada ou habilite a autenticação única (SSO). Para obter mais informações, consulte Fontes de autenticação e Configurar uma fonte de autenticação única (documentação da VMware).

VMware Cloud Disaster Recovery

O VMware Cloud Disaster Recovery (VCDR) (documentação da VMware) é uma solução de recuperação de desastres como serviço (DRaaS) que oferece uma abordagem hierárquica à recuperação de desastres. É possível ajustar os custos e os prazos de objetivo de ponto de recuperação (RPO) e objetivo de tempo de recuperação (RTO) para atender aos requisitos de uma determinada workload. Isso ajuda você a equilibrar a proteção confiável e o uso eficiente de recursos de recuperação de desastres. O VCDR permite:

- Criar backups de máquinas virtuais
- Armazenar backups em armazenamento durável na nuvem
- Escolher entre opções flexíveis de implantação para destinos de restauração, desde sob demanda até standby a quente
- Configurar RPOs e RTOs personalizados

Gerenciar identidades e acessos

Use o VMware Cloud Services Console para gerenciar identidades e acesso ao VMware Cloud Disaster Recovery. O VMware Aria Disaster Recovery usa os mesmos usuários, incluindo identidades federadas e grupos, configurados no VMware Cloud Services Console. Para conceder permissões para esse serviço, é possível atribuir um perfil de serviço do VCDR ou criar um perfil personalizado no VMware Disaster Recovery. Para obter mais informações sobre os perfis de serviço disponíveis, consulte Perfis de serviço do VMware Cloud Disaster Recovery (documentação da VMware).

O VCDR inclui vários perfis integrados que podem ser usados para operar o serviço:

- Administrador: controle total, com exceção de acesso a tokens da API.
- Auditor: acesso somente leitura à interface do usuário, com exceção do gerenciamento de usuários. Acesso a relatórios de conformidade.
- Administrador de DR: permite criar, testar e executar planos de recuperação de desastres.
- Administrador de backup: permite gerenciar sites protegidos e grupos de proteção. Acesso para restaurar VMs.
- Testador de planos: pode criar planos de recuperação de desastres e executar recuperações de teste.
- Administrador do SDDC: pode gerenciar SDDCs.

Recomendações da AWS

Siga as Práticas recomendadas gerais descritas anteriormente neste guia. Não temos recomendações adicionais para gerenciar identidades e acesso neste serviço.

VMware HCX

O VMware HCX (documentação da VMware) é uma plataforma de mobilidade de aplicações que permite a migração de workloads entre SDDCs. O VMware HCX está incluído no VMware Cloud na AWS e pode ser usado para migrar workloads. O VMware HCX permite:

- Configurar malhas de vários sites entre SDDCs
- Estender as redes entre sites do HCX
- Migrar máquinas virtuais

Gerenciar identidades e acessos

Use o VMware vCenter Server para gerenciar identidades e acesso ao VMware HCX. O VMware HCX requer acesso a outros serviços da VMware para criar e gerenciar recursos e migrações, incluindo acesso ao vCenter Server e ao NSX. O VMware HCX tem dois serviços componentes:

- HCX Cloud Manager: no VMware Cloud Services Console, habilite o VMware HCX para o SDDC. Isso instala o dispositivo HCX Cloud Manager no SDDC selecionado. Para obter mais informações, consulte Implantar o HCX Installer OVA no vSphere Client(documentação da VMware). Após a

implantação, é possível usar as credenciais cloudadmin do vCenter Server para acessar o serviço HCX Cloud Manager.

- HCX Connector: é possível obter o arquivo HCX Connector Open Virtualization Archive (OVA) por meio do serviço HCX Cloud Manager. Use esse arquivo para instalar um dispositivo HCX Cloud Manager em qualquer instância do vCenter Server, o que configura essa instância como uma fonte de migração no VMware HCX. Cada instância do HCX Connector tem suas próprias credenciais de administrador e usuário raiz.

Após implantar os dois serviços de componentes, você pode acessar o VMware HCX via vCenter Server. O grupo Administradores do vCenter Single Sign-On recebe automaticamente a atribuição do perfil Administrador do HCX. A instalação do HCX adiciona muitos outros perfis e privilégios ao vCenter Single Sign-On. Use-os para criar controles de acesso minuciosos para o VMware HCX com base nos diferentes tipos de usuários.

Recomendações da AWS

Além das Práticas recomendadas gerais, a AWS recomenda o seguinte ao configurar o VMware HCX para VMware Cloud na AWS:

- Use as regras do Gateway Firewall para restringir o acesso à rede para o serviço HCX Cloud Manager.
- Armazene com segurança as credenciais de administrador e usuário raiz do HCX Connector on-premises. Considere alternar essas credenciais de acordo com as políticas da sua empresa. A VMware gerencia essas credenciais em seu nome para o HCX Cloud Manager.
- Para uma instância on-premises do HCX Connector, considere criar perfis do HCX personalizados que atendam às necessidades de seus diferentes tipos de usuários do HCX. Por exemplo, crie um perfil mais permissivo para usuários que configuram e administram o HCX e crie um perfil menos permissivo para usuários que gerenciam somente migrações.
- Ao emparelhar o VMware HCX com o VMware Cloud na AWS, é necessário utilizar o usuário cloudadmin. Para obter mais informações, consulte a seção Resolução de HCX: diagnóstico de conectividade de emparelhamento de sites (artigo 78340 da Base de Conhecimento da VMware).
- Ao emparelhar o HCX Cloud com o VMware Cloud na AWS, não há suporte à autenticação entre a SDDC do VMware Cloud na AWS e o Active Directory. Para obter mais informações, consulte [VMC na AWS] Ausência de suporte ao AD na configuração do HCX Cloud na nuvem (artigo 90433 da Base de Conhecimento da VMware).

VMware Site Recovery

O VMware Site Recovery (documentação da VMware) é uma solução de recuperação de desastres como serviço (DRaaS) sob demanda baseada no serviço VMware Site Recovery Manager para ambientes on-premises. O VMware Site Recovery permite:

- Implementar replicação, orquestração e automação para ajudar a proteger as workloads em caso de falha no site
- Criar uma solução de recuperação de desastres ponta a ponta para ajudar a proteger os SDDCs

Gerenciar identidades e acessos

Use o VMware vCenter Server para gerenciar identidades e acesso ao VMware Site Recovery. O VMware Site Recovery executa operações em nome dos usuários, por exemplo, replicar ou desligar uma máquina virtual. O Site Recovery usa perfis e privilégios para ajudar a garantir que somente usuários com as permissões corretas possam realizar operações de recuperação, como executar todas as etapas de um plano de recuperação.

Para o Site Recovery, os seguintes perfis de serviço estão disponíveis:

- SrmAdministrator: permite realizar todas as operações de configuração e administração do Site Recovery.
- HmsCloudAdmin: pode listar servidores, mas não pode adicioná-los nem removê-los.

Quando você configura o Site Recovery no VMware Cloud na AWS, as seguintes atualizações de grupos de usuários são configuradas automaticamente:

1. Um novo grupo Administradores do SRM é criado e recebe a atribuição do perfil SrmAdminsitrator.
2. Um novo grupo HmsCloudAdministrators é criado e recebe a atribuição do perfil HmsCloudAdmin.
3. O grupo CloudAdminGroup é adicionado aos grupos Administradores do SRM e HmsCloudAdministrators. Isso fornece ao grupo CloudAdminGroup permissões transitivas para gerenciar o Site Recovery Manager e a replicação do vSphere.

Para obter mais informações, consulte Saiba mais sobre a configuração de permissões para o VMware Site Recovery (documentação da VMware).

Se você usa identidades federadas para acessar o vCenter Server, é necessário usar o Modo vinculado híbrido para adicionar entidades a esses grupos. Para obter mais informações, consulte Configurar o Modo vinculado híbrido (documentação da VMware).

Recomendações da AWS

Além das Práticas recomendadas gerais, a AWS recomenda o seguinte ao configurar o Site Recovery para VMware Cloud na AWS:

- Certifique-se de que os usuários tenham os mesmos perfis nos sites de origem e de destino. Isso garante que objetos protegidos e recuperados tenham permissões idênticas.
- Use o Modo vinculado híbrido para gerenciar as atribuições de perfis do Site Recovery para identidades federadas no vCenter Server.
- O Site Recovery usa endereços IP privados somente dentro do SDDC. De acordo com as Práticas recomendadas gerais, garanta que seu vCenter do VMware Cloud na AWS seja resolvido para um endereço IP privado.

Exemplos de grupos e perfis

A tabela a seguir fornece um exemplo de estratégia de gerenciamento de identidade e acesso para usar o VMware Cloud na AWS. Ela descreve a persona de usuário, os serviços da VMware que ela precisa acessar, a associação à organização e ao grupo, os perfis atribuídos e o tipo de identidade usado (como usuários locais ou identidades federadas). Usando essa tabela como ponto de partida, crie uma estratégia para sua empresa que siga as práticas recomendadas neste guia.

Persona de usuário	Serviços acessados	Nome do grupo de exemplo do VMware Cloud	Perfis de serviço do VMware Cloud	Nome do grupo de exemplo do vCenter Single Sign-On	Perfil do vCenter Single Sign-On	Fonte de identidade
Emergência da organização	VMware Cloud Services Console	Nenhum	Proprietário da organização	Nenhum	Nenhum	Usuário local (endereço de e-mail da conta de serviço)
Administrador da VMware	VMware Cloud Services Console vCenter Server HCX Recuperação do site VCDR	`vmware_admins`	Proprietário da organização	`vmware_admins`	Administrador	Provedor de identidade federado

Persona de usuário	Serviços acessados	Nome do grupo de exemplo do VMware Cloud	Perfis de serviço do VMware Cloud	Nome do grupo de exemplo do vCenter Single Sign-On	Perfil do vCenter Single Sign-On	Fonte de identidade
	vRealizar Operations					
Administrador de backup	vCenter Server	Nenhum	Nenhum	`vmware_backups`	Usuário avançado	Provedor de identidade federado
Administrador de recuperação de desastres	vCenter Server VMware Cloud Services Console Recuperação do site VCDR	`vmware_dr`	Membro da organização Administrador do DR Administrador de DR do SDDC	`vmware_dr`	SrmAdministrator HmsCloudAdmin	Provedor de identidade federado

Persona de usuário	Serviços acessados	Nome do grupo de exemplo do VMware Cloud	Perfis de serviço do VMware Cloud	Nome do grupo de exemplo do vCenter Single Sign-On	Perfil do vCenter Single Sign-On	Fonte de identidade
Operador do VMware	VMware Cloud Services Console vCenter Server HCX vRealizar Operations	`vmware_ops`	Membro da organização Administrador de vROps	`vmware_ops`	Usuário avançado	Provedor de identidade federado
Equipe de redes	VMware Cloud Services Console vCenter Server	`vmware_networks`	Membro da organização Administrador do NSX Cloud	`vmware_networks`	Readonly	Provedor de identidade federado

Persona de usuário	Serviços acessados	Nome do grupo de exemplo do VMware Cloud	Perfis de serviço do VMware Cloud	Nome do grupo de exemplo do vCenter Single Sign-On	Perfil do vCenter Single Sign-On	Fonte de identidade
Equipe de segurança	VMware Cloud Services Console vCenter Server HCX (acesso temporário) Recuperação do site VCDR vRealizar Operations	`vmware_security`	Membro da organização vROps ReadOnly	`vmware_security`	Readonly	Provedor de identidade federado
Auditores	VMware Cloud Services Console vCenter Server	`vmware_audit`	Membro da organização	`vmware_audit`	Readonly	Provedor de identidade federado

Próximas etapas

Este guia abordou as práticas recomendadas que recomendamos para gerenciar a identidade e o acesso ao VMware Cloud na AWS e serviços relacionados da VMware. Essas recomendações foram desenvolvidas não só para ajudar você a proteger sua infraestrutura de nuvem e nuvem híbrida e impedir acessos não autorizados, mas também para serem escaláveis e eficientes. Ao atribuir usuários a grupos e depois atribuir perfis a grupos, é possível conceder ou restringir permissões com mais rapidez e minimizar a sobrecarga associada à configuração de usuários individuais. Além disso, ao usar federação para um provedor de identidade externo e o vCenter Single Sign-On, é possível fornecer uma experiência perfeita de autenticação única para seus usuários.

Use a tabela Exemplos de grupos e perfis para começar a criar uma estratégia de gerenciamento de identidade e acesso que funcione para sua empresa. Depois de revisar as recomendações deste guia, sugerimos revisar os links fornecidos na seção Recursos. Esses recursos ajudarão você a aprender mais sobre os serviços de nuvem da VMware e como configurar as práticas recomendadas descritas neste guia.

Recursos

Recursos relacionados do AWS

- Visão geral e modelo operacional do VMware Cloud na AWS
- Opções de recuperação de desastres para workloads no VMware Cloud na AWS
- Configurar opções de descarregamento de armazenamento para VMware Cloud na AWS
- Implementar um SDDC VMware na AWS usando o VMware Cloud na AWS
- Migrar um SDDC VMware para o VMware Cloud na AWS usando o VMware HCX

Documentação da VMware

VMware Cloud na AWS

- Configurar a federação corporativa para serviços na nuvem
- Gerenciamento de identidade e acesso para VMware Cloud Services

VMware vCenter Server e vCenter Single Sign-On

- Entender a autorização no vSphere
- Administração do vSphere no VMware Cloud na AWS
- Autenticação do vSphere com vCenter Single Sign-On
- Configurar as fontes de identidade do vCenter Single Sign-On
- Herança hierárquica de permissões
- Segurança e acesso a informações para o vCenter Server
- Privilégios necessários do vSphere para tarefas comuns

VMware NSX

- Guia de administração do NSX
- Segurança e acesso às informações para o NSX-T Data Center

VMware HCX

- Guia do usuário do VMware HCX
- Requisitos de contas e perfis de usuário do VMware HCX

Suíte VMware Aria e vRealize

- Documentação do VMware vRealize Operations
- Perfis e privilégios no vRealize Operations Cloud
- Folha de dados do VMware vRealize Log Insight
- Introdução às operações do VMware Aria for Logs
- Guia do VMware Cloud Services
- Gerenciamento de usuários no vRealize Network Insight

VMware Site Recovery

- Documentação do VMware Site Recovery
- Privilégios, perfis e permissões do Site Recovery Manager
- Configuração de permissão para o VMware Site Recovery no VMware Cloud na AWS

VMware Cloud Disaster Recovery

- Perfis de usuário do VMware Cloud Disaster Recovery

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
Acesso ao VMware HCX	Atualizamos as Recomendações da AWS para configurar o VMware HCX para VMware Cloud na AWS.	5 de junho de 2023
Publicação inicial	—	3 de novembro de 2022

Glossário de Recomendações da AWS

Os termos a seguir são comumente usados em estratégias, guias e padrões fornecidos pelas Recomendações da AWS. Para sugerir entradas, use o link Fornecer feedback no final do glossário.

Números

7 Rs

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

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Aurora Edição Compatível com PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Relational Database Service (Amazon RDS) para Oracle na AWS Cloud.
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migrar seu sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: migrar seu banco de dados Oracle on-premises para o Oracle em uma instância do EC2 na AWS Cloud.
- 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. Esse cenário de migração é específico para o VMware Cloud na AWS, o qual oferece suporte a compatibilidade de máquina virtual (VM) e portabilidade de workloads entre seu ambiente on-premises e a AWS. É possível usar as tecnologias VMware Cloud Foundation de seus datacenters on-premises ao migrar sua infraestrutura para o VMware Cloud na AWS. Exemplo: realocar o hipervisor que hospeda seu banco de dados Oracle para o VMware Cloud na AWS.

- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.
- Retirar: desative ou remova aplicações que não são mais necessárias em seu ambiente de origem.

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja a inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade (ACID)

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

controle de acesso por atributo (ABAC)

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

fonte de dados autorizada

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

zona de disponibilidade

Um local distinto em uma Região da AWS que é isolado das falhas em outras zonas de disponibilidade e fornece conectividade de rede de baixa latência e baixo custo para outras zonas de disponibilidade na mesma região.

AWS Cloud Adoption Framework (AWS CAF)

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

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

AWS Workload Qualification Framework (AWS WQF)

Uma ferramenta que avalia os workloads de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS A WQF é fornecida com o 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

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

ramo

Uma área contida de um repositório de código. A primeira ramificação criada em um repositório é a ramificação principal. Você pode criar uma nova ramificação a partir de uma ramificação

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

acesso em vidro quebrado

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

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.

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja a integração e a entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de Excelência da Nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as publicações da CCoE no blog de Estratégia Empresarial na AWS Cloud.

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 ao migrar para a AWS Cloud:

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação: realizar investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma zona de pouso, definir um CCoE, 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 publicação no blog A jornada rumo à nuvem em primeiro lugar e os estágios da adoção no Blog de estratégia empresarial na AWS Cloud. Para obter informações sobre como eles se relacionam com a estratégia de migração da AWS, 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 ouAWS 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

Um campo da IA utilizado por máquinas para identificar pessoas, lugares e coisas em imagens com precisão igual ou superior aos níveis humanos. Geralmente construído com modelos de aprendizado profundo, ele automatiza a extração, análise, classificação e compreensão de informações úteis de uma única imagem ou sequência de imagens.

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

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.

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

Uma abordagem de segurança da informação na qual uma série de mecanismos e controles de segurança são cuidadosamente distribuídos por toda a rede de computadores para proteger a confidencialidade, a integridade e a disponibilidade da rede e dos dados nela contidos. Ao adotar essa estratégia na AWS, você adiciona vários controles em diferentes camadas da estrutura

do AWS Organizations para ajudar a proteger os recursos. Por exemplo, uma defense-in-depth abordagem pode combinar autenticação multifatorial, segmentação de rede e criptografia.

administrador delegado

No AWS Organizations, um serviço compatível pode registrar uma conta-membro da AWS para administrar as contas da organização e gerenciar permissões para esse serviço. Essa conta é chamada de administrador delegado para esse serviço Para obter mais informações e uma lista de serviços compatíveis, consulte Serviços que funcionam com o AWS Organizations na documentação do AWS Organizations.

implantação

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

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

recuperação de desastres (DR)

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 em workloads na AWS: Recuperação na Nuvem na Documentação do Well-Architected Framework AWS.

DML

Veja a linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja a recuperação de desastres.

detecção de deriva

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

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

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 pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. É possível criar um serviço de endpoint com o AWS PrivateLink e conceder permissões a outras Contas da AWS ou a entidades principais do AWS Identity and Access Management (IAM). Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais

informações, consulte Criar um serviço de endpoint na documentação do Amazon Virtual Private Cloud (Amazon VPC).

criptografia envelopada

O processo de criptografar uma chave de criptografia com outra chave de criptografia. Para obter mais informações, consulte Criptografia envelopada na documentação do 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 epics de segurança da AWS CAF incluem gerenciamento de identidade e acesso, controles detectivos, 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.

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

NoNuvem 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 gerenciar recursos, políticas e conformidade em todas as unidades organizacionais (UOs). Barreiras de proteção preventivas impõem políticas para

garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usandoAWS Config,AWS Security Hub, Amazon GuardDutyAWS Trusted Advisor, Amazon Inspector e verificações personalizadasAWS 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 compartilha o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server para Amazon RDS para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

dados quentes

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

hotfix

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

período de hipercuidados

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

I

IaC

Veja a infraestrutura como código.

Política baseada em identidade

Uma política associada a uma ou mais entidades principais do IAM que define suas permissões dentro do ambiente da Nuvem AWS.

aplicação ociosa

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

IIoT

Veja a Internet das Coisas industrial.

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que infraestruturas mutáveis. Para

obter mais informações, consulte as melhores práticas de implantação usando infraestrutura imutável no Well-Architected AWS Framework.

VPC de entrada (admissão)

Em uma arquitetura de várias contas da AWS, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de uma aplicação. A Arquitetura de referência de segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação 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.

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 das Coisas Industrial (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 Construir uma estratégia de transformação digital para a Internet das Coisas Industrial (IIoT).

VPC de inspeção

Em uma arquitetura de várias contas da AWS, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (na mesma ou em diferentes Regiões da AWS), na Internet e em redes on-premises. A Arquitetura de referência de segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação 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 machine learning com a AWS.

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

Uma zona de pouso é um ambiente da AWS com várias contas que é bem arquitetado, 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 do IAM.

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

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

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.

serviços gerenciados

Serviços da AWSpara 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.

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

Todas as Contas da AWS, exceto a conta de gerenciamento que faz parte de uma organização no AWS Organizations. Uma conta só pode ser membro de uma organização de cada vez.

microsserviço

Um serviço pequeno e independente que se comunica por meio de APIs bem definidas e normalmente pertence a equipes pequenas e autônomas. 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 Integrar microsserviços usando serviços da AWS sem 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 APIs leves. 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 Implementar microsserviços na AWS.

Programa de Aceleração da Migração (MAP)

Um programa da AWS que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a

compensar o custo inicial das migrações. O MAP inclui uma metodologia de migração para executar migrações legadas de forma metódica e um conjunto de ferramentas para automatizar e acelerar cenários comuns de migração.

migração em escala

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

fábrica de migração

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

metadados de migração

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

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: redefina a hospedagem da migração para o Amazon EC2 com o Application Migration Service da AWS.

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

A abordagem usada para migrar um workload para a AWS Cloud. 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.

MAPA

Consulte Avaliação do portfólio de migração.

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 aplicações na AWS Cloud.

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 Avaliar a preparação para modernização de aplicações na AWS Cloud.

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.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja o controle de acesso de origem.

CARVALHO

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

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

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

Um método de migração no qual a workload de origem é copiada para o sistema de destino sem ser colocada offline. As aplicações conectadas à workload podem continuar funcionando durante

a migração. Esse método envolve um tempo de inatividade nulo ou mínimo e normalmente é usado para workloads essenciais para a produção.

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

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 pelo AWS CloudTrail que registra todos os eventos para todas asContas da AWS em uma organização no AWS Organizations. Essa trilha é criada em cada Conta da AWS que faz parte da organização e monitora a atividade em cada conta. Para obter mais informações, consulte Criação de uma trilha para uma organização na CloudTrail documentação.

gerenciamento de alterações organizacionais (OCM)

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

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

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

OU

Veja a análise de prontidão operacional.

VPC de saída (egresso)

Em uma arquitetura de várias contas da AWS, uma VPC que lida com conexões de rede que são iniciadas de dentro de uma aplicação. A Arquitetura de referência de segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

P

limite de permissões

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

informações de identificação pessoal (PII)

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

PII

Veja as informações de identificação pessoal.

manual

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

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.

entidade principal

Entidade na AWS que pode executar ações e acessar recursos. Essa entidade geralmente é um usuário raiz de uma Conta da AWS, um perfil do IAM ou um usuário. Para obter mais

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

Privacidade por design

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

zonas hospedadas privadas

Um contêiner que armazena informações sobre como você quer que o Amazon Route 53 responda a consultas ao DNS para um domínio e seus subdomínios dentro de uma 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.

ambiente de produção

Veja o ambiente.

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.

Q

plano de consulta

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

regressão de planos de consultas

Quando um otimizador de serviço de banco de dados escolhe um plano menos adequado do que escolhia antes de uma determinada alteração no ambiente de banco de dados ocorrer. Isso pode

ser causado por alterações em estatísticas, restrições, configurações do ambiente, associações de parâmetros de consulta e atualizações do mecanismo de banco de dados.

R

Matriz RACI

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

ransomware

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

Matriz RASCI

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

RCAC

Veja o controle de acesso por linha e coluna.

réplica de leitura

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

rearquiteta

Veja 7 Rs.

objetivo de ponto de recuperação (RPO)

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

refatorar

Veja 7 Rs.

região

Uma coleção de recursos da AWS em uma área geográfica. Cada Região da AWS é isolada e independente das demais para fornecer tolerância a falhas, estabilidade e resiliência. Para obter mais informações, consulte Gerenciar Regiões da AWS na Referência geral da AWS.

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.

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

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

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

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

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite a autenticação única (SSO) federada para que os usuários possam fazer login no AWS

Management Console ou chamar as operações de API da AWS sem que você precise criar um usuário no IAM para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte Sobre a federação baseada em SAML 2.0 na documentação do IAM.

SCP

Veja a política de controle de serviços.

secret

EmAWS 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 Secret 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 sistema SIEM coleta, monitora e analisa dados de servidores, redes, dispositivos e outras fontes para detectar ameaças e violações de segurança e gerar alertas.

automação de resposta de segurança

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

Criptografia do lado do servidor

A criptografia dos dados no destino pelo AWS service (Serviço da AWS) que os recebe.

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização no AWS Organizations. As SCPs definem barreiras de proteção ou estabelecem limites para as ações que um administrador pode delegar a usuários ou perfis. É possível usar SCPs como listas de permissão ou de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte Políticas de controle de serviços na documentação do AWS Organizations.

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

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

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

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

CUSPE

Veja um único ponto de falha.

esquema de estrelas

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

padrão strangler fig

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

sub-rede

Um intervalo de endereços IP na VPC. Uma sub-rede deve residir em uma única zona de disponibilidade.

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 valor chave que atuam como metadados para organizar seus recursos do 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 pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações, consulte O que é um gateway de trânsito? na documentação do AWS Transit Gateway.

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 no 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 Como usar o AWS Organizations com outros serviços da AWS na documentação do AWS Organizations.

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

Um conceito que se refere a informações imprecisas, incompletas ou desconhecidas que podem minar a confiabilidade dos modelos preditivos de ML. Há dois tipos de incertezas: a incerteza epistêmica é causada por dados limitados e incompletos, enquanto a incerteza aleatória é

causada pelo ruído e pela aleatoriedade inerentes aos dados. Para obter mais informações, consulte o guia Como quantificar a incerteza em sistemas de aprendizado profundo.

tarefas indiferenciadas

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

ambientes superiores

Veja o ambiente.

V

aspiração

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

controle de versões

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

emparelhamento de VPC

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

vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte o AWS Workload Qualification Framework.

escreva uma vez, leia muitas (WORM)

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

Z

exploração de dia zero

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

vulnerabilidade de dia zero

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

aplicação zumbi

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

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