AWS Linha de base de segurança de inicialização (AWS SSB)

AWS Orientação prescritiva

AWS Orientação prescritiva: AWS Linha de base de segurança de inicialização (AWS SSB)

Table of Contents

AWS Startup Security Baseline (AWS SSB)

Jay Michael, Amazon Web Services (AWS)

Maio de 2023 (histórico do documento)

O AWS Startup Security Baseline (SSB) é um conjunto de controles que cria uma base mínima para as empresas criarem com segurança na AWS sem diminuir sua agilidade. Esses controles formam a base de sua postura de segurança e se concentram em proteger as credenciais, permitir o registro e a visibilidade, gerenciar informações de contato e implementar limites básicos de dados.

Os controles deste guia foram projetados pensando nas startups que estão realmente começando com o objetivo de mitigar os riscos de segurança mais comuns sem exigir um esforço significativo. Muitas startups começam sua jornada na Nuvem AWS com uma única Conta da AWS. À medida que as organizações crescem, elas migram para arquiteturas de várias contas. As orientações neste guia foram feitas para arquiteturas de conta única, mas ajudam a configurar controles de segurança que são facilmente migrados ou modificados à medida que você faz a transição para uma arquitetura de várias contas.

Os controles no AWS SSB são separados em duas categorias: conta e workload. Os controles de conta ajudam a manter sua conta da AWS segura. Eles incluem recomendações para configurar o acesso, as políticas e as permissões do usuário, além de recomendações sobre como monitorar sua conta em busca de atividades não autorizadas ou potencialmente maliciosas. Os controles de workload ajudam a proteger seus recursos e código na nuvem, como aplicações, processos de back-end e dados. Eles incluem recomendações como criptografia e redução do escopo de acesso.

> **Note**
>
> Alguns dos controles recomendados neste guia substituem os padrões configurados durante a configuração inicial, enquanto a maioria define novas configurações e políticas. Este documento não deve, de forma alguma, ser considerado abrangente para todos os controles disponíveis.

Público-alvo

Este guia é mais adequado para startups que estão nos estágios iniciais de desenvolvimento, com equipe e operações mínimas.

Startups ou outras empresas que estão em estágios posteriores de operação e crescimento ainda podem obter um valor significativo ao revisar esses controles em comparação com suas práticas atuais. Se você identificar alguma lacuna, poderá implementar os controles individuais neste guia e, em seguida, avaliá-los quanto à adequação como uma solução de longo prazo.

> **Note**
>
> Os controles recomendados neste guia são fundamentais por natureza. Startups ou outras empresas que operam em um estágio posterior de escala ou sofisticação devem adicionar controles adicionais conforme aplicável.

Estrutura básica e responsabilidades de segurança

O AWS Well-Architected ajuda os arquitetos de nuvem a criar uma infraestrutura de alta performance que é segura, resiliente e eficiente para suas aplicações e workloads. O AWS Startup Security Baseline se alinha ao pilar de segurança do AWS Well-Architected Framework. O pilar de segurança descreve como aproveitar as tecnologias de nuvem para proteger dados, sistemas e ativos de uma forma que possa melhorar sua postura de segurança. Isso ajuda você a atender aos seus requisitos comerciais e regulatórios conforme as recomendações atuais da AWS.

Você pode avaliar sua adesão às práticas recomendadas do Well-Architected com o AWS Well-Architected Tool em sua conta da AWS.

Segurança e conformidade são uma responsabilidade compartilhada entre a AWS e o cliente. O modelo de responsabilidade compartilhada é frequentemente descrito dizendo que a AWS é responsável pela segurança da nuvem (ou seja, por proteger a infraestrutura que executa todos os serviços oferecidos na Nuvem AWS) e você é responsável pela segurança na nuvem (conforme determinado pelos serviços da Nuvem AWS que você seleciona). No modelo de responsabilidade compartilhada, implementar os controles de segurança neste documento faz parte de sua responsabilidade como cliente.

Como proteger sua conta

Os controles e recomendações nesta seção ajudam a manter sua AWS conta segura. Ele enfatiza o uso AWS Identity and Access Management (IAM) de usuários, grupos de usuários e funções (também conhecidos como diretores) para acesso humano e de máquina, restringindo o uso do usuário raiz e exigindo autenticação multifatorial. Nesta seção, você confirma que AWS tem as informações de contato necessárias para entrar em contato com você sobre a atividade e o status da sua conta. Você também configura serviços de monitoramento, como AWS Trusted Advisor Amazon e GuardDuty AWS Budgets, para ser notificado sobre atividades em sua conta e poder responder rapidamente se a atividade não for autorizada ou inesperada.

Esta seção contém os seguintes tópicos:

ACCT.01: definir contatos em nível de conta para listas de distribuição de e-mail válidas

Ao configurar contatos principais e alternativos para sua AWS conta, use uma lista de distribuição de e-mail em vez do endereço de e-mail de uma pessoa. O uso de uma lista de distribuição de e-mail garante que a propriedade e a acessibilidade sejam preservadas à medida que as pessoas entram e saem da sua organização. Defina contatos alternativos para notificações de faturamento, operações

e segurança e use as listas de distribuição de e-mail apropriadas adequadamente. AWS usa esses endereços de e-mail para entrar em contato com você, por isso é importante que você mantenha o acesso a eles.

Para editar o nome da conta, a senha do usuário raiz ou o endereço de e-mail do usuário raiz

1. Faça login na página Configurações da conta no console de Gerenciamento de Faturamento e Custos em https://console.aws.amazon.com/billing/home?#/account.
2. Na página Account Settings, ao lado de Account Settings, escolha Edit.
3. Ao lado do campo que você deseja atualizar, escolha Editar.
4. Depois de fazer as alterações, escolha Save changes.
5. Depois de fazer as alterações, selecione Done (Concluído).

Para editar suas informações de contato

1. Na página Configurações da conta, em Informações de contato, escolha Editar.
2. Para os campos que deseja alterar, insira as informações atualizadas e escolha Atualizar.

Para adicionar, atualizar ou remover contatos alternativos

1. Na página Configurações da conta, em Contatos alternativos, escolha Editar.
2. Para os campos que deseja alterar, insira as informações atualizadas e escolha Atualizar.

ACCT.02: restringir o uso do usuário raiz

O usuário root é criado quando você se inscreve em uma AWS conta, e esse usuário tem privilégios e permissões de propriedade total sobre a conta que não podem ser alterados. Use o usuário raiz para as tarefas específicas que o exigem. Para obter mais informações, consulte Tarefas que exigem credenciais de usuário raiz (AWS Account Management). Execute todas as outras ações em sua conta usando outros tipos de identidades do IAM, como usuários federados com perfis do IAM. Para obter mais informações, consulte credenciais de segurança da AWS (documentação do IAM).

Para restringir o uso do usuário raiz

1. Exija a autenticação multifator (MFA) para o usuário raiz, conforme descrito em ACCT.05: exigir autenticação multifator (MFA) para login.

2. Crie um usuário administrativo para não precisar usar o usuário raiz nas tarefas do dia a dia. Para obter mais informações sobre como configurar o acesso de usuários, consulte ACCT.03: configurar o acesso ao console para cada usuário.

ACCT.03: configurar o acesso ao console para cada usuário

Como prática recomendada, AWS recomenda o uso de credenciais temporárias para conceder acesso Contas da AWS e recursos. As credenciais temporárias têm duração limitada. Por isso, não será necessário alterná-las ou revogá-las explicitamente quando elas não forem mais necessárias. Para obter mais informações, consulte Credenciais de segurança temporárias (documentação do IAM).

Para usuários humanos, AWS recomenda usar identidades federadas de um provedor de identidade centralizado (IdP), como AWS IAM Identity Center Okta, Active Directory ou Ping Identity. A federação de usuários permite que você defina identidades em um único local central, e os usuários podem se autenticar com segurança em vários aplicativos e sites AWS, inclusive usando apenas um conjunto de credenciais. Para obter mais informações, consulte Federação de identidades no AWS IAM Identity Center (AWS site).

> **Note**
>
> A federação de identidades pode complicar a transição de uma arquitetura de conta única para uma arquitetura de várias contas. É comum que as startups adiem a implementação da federação de identidades até que tenham estabelecido uma arquitetura de várias contas gerenciada na AWS Organizations.

Para configurar a federação de identidades

1. Se estiver usando o IAM Identity Center, consulte Introdução (documentação do IAM Identity Center).

   Se estiver usando um IdP externo ou de terceiros, consulte Criar provedores de identidade do IAM (documentação do IAM).
2. Certifique-se de que seu IdP aplique a autenticação multifator (MFA).
3. Aplique permissões de acordo com ACCT.04: atribuir permissões.

Para startups que não estão preparadas para configurar a federação de identidades, é possível criar usuários diretamente no IAM. Essa não é uma prática recomendada de segurança porque essas são credenciais de longo prazo que nunca expiram. No entanto, é uma prática comum para startups em início de operação para evitar dificuldades na transição para uma arquitetura de várias contas quando estiverem operacionalmente prontas.

Como base, é possível criar um usuário do IAM para cada pessoa que precisa acessar o AWS Management Console. Se você configurar usuários do IAM, não compartilhe credenciais entre usuários e alterne regularmente as credenciais de longo prazo.

> **Warning**
>
> Os usuários do IAM têm credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários.

Para criar um usuário do IAM

1. Crie usuários do IAM (documentação do IAM).
2. Aplique permissões de acordo com ACCT.04: atribuir permissões.

ACCT.04: atribuir permissões

Configure as permissões do usuário na conta atribuindo políticas à sua identidade do IAM (grupo de usuários ou perfil). Você pode personalizar as permissões ou anexar políticas AWS gerenciadas, que são políticas autônomas projetadas AWS para fornecer permissões para muitos casos de uso comuns. Se você personalizar as permissões, siga as práticas recomendadas de segurança de concessão de privilégio mínimo. Privilégio mínimo é a prática de conceder o conjunto mínimo de permissões que cada usuário precisa para realizar suas tarefas.

Se você estiver usando identidades federadas, os usuários acessarão a conta assumindo um perfil do IAM por meio do provedor de identidades externo. A função do IAM define o que os usuários autenticados pelo IdP da sua organização podem fazer. AWS Você aplica políticas personalizadas ou AWS gerenciadas a essa função para configurar permissões.

Para atribuir permissões para identidades federadas

- Se você estiver usando o IAM Identity Center, consulte Usar políticas do IAM em conjuntos de permissões (documentação do IAM Identity Center).

  Se estiver usando um IdP externo ou de terceiros, consulte Adicionar permissões de identidade do IAM (documentação do IAM).

Se estiver usando usuários do IAM, você poderá usar grupos de usuários ou perfis para gerenciar permissões para vários usuários do IAM. Recomendamos grupos de usuários para startups porque eles são mais fáceis de gerenciar e menos propensos a configurações incorretas que podem representar riscos de segurança para sua conta. Atribua usuários a grupos de usuários baseados em suas funções no trabalho. Exemplos de grupos de usuários incluem engenheiros de aplicativos, dados, redes e operações de desenvolvimento (DevOps). Os tipos de usuários também podem ser divididos em grupos menores com base na autoridade de tomada de decisão, por exemplo, engenheiros seniores e não seniores.

Para atribuir permissões a usuários do IAM

1. Crie grupos de usuários do IAM (documentação do IAM).
2. Anexe uma política AWS gerenciada a um grupo de usuários do IAM (documentação do IAM).

ACCT.05: exigir autenticação multifator (MFA) para login

Com a MFA, os usuários têm um dispositivo que gera uma resposta a um desafio de autenticação. As credenciais de cada usuário e a resposta gerada pelo dispositivo são necessárias para concluir o processo de login. Como prática recomendada de segurança, habilite o MFA para Conta da AWS acesso, especialmente para credenciais de longo prazo, como o usuário raiz da conta e os usuários do IAM.

Para configurar a MFA para o usuário raiz

1. Faça login no AWS Management Console athttps://console.aws.amazon.com/.
2. No lado direito da barra de navegação, selecione seu nome de conta e selecione Minhas credenciais de segurança.
3. Se necessário, selecione Continuar para as credenciais de segurança.
4. Expanda a seção Autenticação multifator (MFA).

5. Selecione Activate MFA (Ativar MFA).
6. Siga as instruções do assistente para configurar seus dispositivos de MFA adequadamente. Para obter mais informações, consulte Habilitar dispositivos de MFA para usuários na AWS (documentação do IAM).

Para configurar a MFA no IAM Identity Center

- Habilitar a MFA (documentação do IAM Identity Center)

Para configurar a MFA para seu próprio usuário do IAM

1. Usando as credenciais de acesso, faça login no console do IAM em https://console.aws.amazon.com/iam.
2. Na barra de navegação no canto superior direito, selecione seu nome de usuário e selecione My Security Credentials (Minhas credenciais de segurança).
3. Na guia AWS IAM credentials (Credenciais do AWS IAM), na seção Multi-factor authentication (Autenticação multifator), escolha Manage MFA device (Gerenciar dispositivo com MFA).

Para configurar a MFA para outros usuários do IAM

1. Faça login no AWS Management Console e abra o console do IAM emhttps://console.aws.amazon.com/iam.
2. No painel de navegação, escolha Users.
3. Selecione o nome do usuário para o qual você deseja habilitar a MFA e selecione a guia Security credentials (Credenciais de segurança).
4. Ao lado de Dispositivo MFA atribuído, escolha Gerenciar.
5. Siga as instruções do assistente para configurar seus dispositivos de MFA adequadamente. Para obter mais informações, consulte Habilitar dispositivos de MFA para usuários na AWS (documentação do IAM).

ACCT.06: aplicar uma política de senha

Os usuários fazem login no AWS Management Console fornecendo credenciais de login, e o MFA é recomendado. Exija que as senhas sigam uma política de senha forte para ajudar a evitar descobertas por meio de força bruta ou engenharia social.

Para obter mais informações sobre as recomendações mais recentes para senhas fortes, consulte o Guia de política de senhas no site do Center for Internet Security (CIS).

Para usuários do IAM, é possível configurar os requisitos de senha em uma política de senha personalizada do IAM. Para obter mais informações, consulte Definir uma política de senha para contas (documentação do IAM).

Para criar uma política de senha personalizada

1. Faça login no AWS Management Console e abra o console do IAM emhttps://console.aws.amazon.com/iam.
2. No painel de navegação, selecione Configurações da conta.
3. Na seção Política de senha, escolha Change password policy (Alterar política de senha).
4. Selecione as opções que deseja aplicar à política de senhas e escolha Salvar alterações.

ACCT.07 — Entregar CloudTrail registros para um bucket S3 protegido

As ações realizadas por usuários, funções e serviços em sua AWS conta são registradas como eventos em AWS CloudTrail. CloudTrail está ativado por padrão e, no CloudTrail console, você pode acessar 90 dias de informações do histórico de eventos. Para visualizar, pesquisar, baixar, arquivar, analisar e responder à atividade da conta em toda a sua AWS infraestrutura, consulte Visualização de eventos com histórico de CloudTrail eventos (CloudTrail documentação).

Para reter o CloudTrail histórico além de 90 dias com dados adicionais, você cria uma nova trilha que entrega arquivos de log em um bucket do Amazon Simple Storage Service (Amazon S3) para todos os tipos de eventos. Ao criar uma trilha no CloudTrail console, você cria uma trilha multirregional.

Para criar uma trilha que entregue registros de todos em um Regiões da AWS bucket do S3

1. Crie uma trilha (CloudTrail documentação). Na página Escolher eventos de log, faça o seguinte:
    a. Para Atividade da API, escolha Leitura e Gravação.
    b. Para ambientes de pré-produção, escolha Excluir eventos da AWS KMS . Isso exclui todos os AWS Key Management Service (AWS KMS) eventos da sua trilha. AWS KMS lê ações como`Encrypt`,`Decrypt`, e `GenerateDataKey` pode gerar um grande volume de eventos.

Para ambientes de produção, escolha a opção de registrar eventos de gerenciamento de Gravação e desmarque a caixa de seleção de Excluir eventos do AWS KMS . Isso exclui eventos de AWS KMS leitura de alto volume, mas ainda registra eventos de gravação relevantes`Disable`, como`Delete`, e. `ScheduleKey` Essas são as configurações mínimas de AWS KMS registro recomendadas para um ambiente de produção.

2. A nova trilha será exibida na página Trails (Trilhas). Em cerca de 15 minutos, CloudTrail publica arquivos de log que mostram as chamadas da interface de programação de AWS aplicativos (API) feitas em sua conta. Você pode ver os arquivos de log no bucket do S3 que você especificou.

Para ajudar a proteger os buckets do S3 onde você armazena CloudTrail os arquivos de log

1. Revise a política de bucket do Amazon S3 (CloudTrail documentação) para todo e qualquer bucket em que você armazena arquivos de log e ajuste-a conforme necessário para remover qualquer acesso desnecessário.
2. Como prática recomendada de segurança, certifique-se de adicionar manualmente uma chave de condição do `aws:SourceArn` para a política de bucket. Para obter mais informações, consulte Criar ou atualizar um bucket do Amazon S3 para usar para armazenar os arquivos de log de uma trilha organizacional (CloudTrail documentação).
3. Habilite a exclusão da MFA (documentação do Amazon S3).

ACCT.08: impedir o acesso público a buckets do S3 privados

Por padrão, somente o usuário raiz do Conta da AWS e o principal do IAM, se usados, têm permissões para ler e gravar nos buckets do Amazon S3 criados por esse principal. As entidades principais adicionais do IAM recebem acesso por meio de políticas baseadas em identidade, e as condições de acesso podem ser aplicadas por uma política de bucket. É possível criar políticas de bucket que concedam ao público geral acesso ao bucket, um bucket público.

Os buckets criados em ou após 28 de abril de 2023 têm a configuração Bloquear acesso público habilitada por padrão. Para buckets criados antes dessa data, os usuários podem configurar incorretamente a política de bucket e, sem querer, conceder acesso ao público. Você pode evitar essa configuração incorreta habilitando a configuração Bloquear acesso público para cada bucket. Se você não tiver casos de uso atuais ou futuros para um bucket público do S3, habilite essa

configuração no Conta da AWS nível. Essa configuração impede políticas que permitem acesso público.

Para impedir o acesso público a buckets do S3

- Configure o bloqueio de acesso público para seus buckets do S3 (documentação do Amazon S3).

AWS Trusted Advisor gera uma descoberta amarela para buckets do S3 que permite acesso de lista ou leitura ao público e gera uma descoberta vermelha para buckets que permitem uploads ou exclusões públicas. Como linha de base, siga o controle ACCT.12: monitorar e resolver problemas de alto risco usando o Trusted Advisor para identificar e corrigir buckets mal configurados. Os buckets do S3 acessíveis ao público também são indicados no console do Amazon S3.

ACCT.09: excluir VPCs, sub-redes e grupos de segurança não utilizados

Para reduzir a oportunidade de problemas de segurança, exclua ou desative recursos que não estão sendo usados. Em uma nova AWS conta, por padrão, uma nuvem privada virtual (VPC) é criada automaticamente em cada uma Região da AWS, o que permite atribuir endereços IP públicos em sub-redes públicas. No entanto, se essas VPCs não forem necessárias, isso representará um risco de exposição não intencional de recursos.

Se elas não estiverem em uso, exclua as VPCs padrão em todas as regiões, e não apenas aquelas nas regiões em que você pode implantar workloads. A exclusão de uma VPC também exclui seus componentes, como sub-redes e grupos de segurança.

> **Note**
>
> É possível visualizar todas as regiões e VPCs no console do Amazon EC2 Global View em https://console.aws.amazon.com/ec2globalview/home. Para obter mais informações, consulte Listar e filtrar recursos entre regiões usando o Amazon EC2 Global View (documentação do Amazon EC2).

Para excluir VPCs padrão não utilizadas

1. Exclua sua VPC (documentação da Amazon VPC).

2. Repita conforme necessário para VPCs em outras regiões.

ACCT.10 — Configure AWS Budgets para monitorar seus gastos

AWS Budgets permita o monitoramento dos custos mensais e do uso com notificações quando se prevê que os custos excedam os limites desejados. As notificações de custos previstos podem fornecer uma indicação de atividade inesperada, fornecendo defesa extra, além de outros sistemas de monitoramento, como AWS Trusted Advisor o Amazon GuardDuty. Monitorar e entender seus AWS custos também faz parte de uma boa higiene operacional.

Para configurar um orçamento em AWS Budgets

- Crie um orçamento de custo (AWS Budgets documentação).

ACCT.11 — Ativar e responder às notificações GuardDuty

GuardDuty A Amazon é um serviço de detecção de ameaças que monitora continuamente comportamentos maliciosos ou não autorizados para ajudar a proteger suas AWS contas, cargas de trabalho e dados. Quando detecta atividades inesperadas e potencialmente maliciosas, GuardDuty fornece descobertas de segurança detalhadas para visibilidade e remediação. GuardDuty pode detectar ameaças como atividades de mineração de criptomoedas, acesso de clientes e retransmissões do Tor, comportamento inesperado e credenciais do IAM comprometidas. Habilite GuardDuty e responda às descobertas para impedir comportamentos potencialmente maliciosos ou não autorizados em seu AWS ambiente. Para obter mais informações sobre descobertas em GuardDuty, consulte Tipos de busca (GuardDuty documentação).

Você pode usar o Amazon CloudWatch Events para configurar notificações automáticas ao GuardDuty criar uma descoberta ou a descoberta mudar. Primeiro, configure um tópico do Amazon Simple Notification Service (Amazon SNS) e adicione endpoints ou endereços de e-mail para o tópico. Em seguida, você configura um CloudWatch evento para GuardDuty descobertas, e a regra do evento notifica os endpoints no tópico do Amazon SNS.

Para habilitar GuardDuty e GuardDuty notificações

1. Habilite a Amazon GuardDuty (GuardDuty documentação).
2. Crie uma regra de CloudWatch eventos para notificá-lo das GuardDuty descobertas (GuardDutydocumentação).

ACCT.12: monitorar e resolver problemas de alto risco usando o Trusted Advisor

AWS Trusted Advisor examina passivamente sua AWS infraestrutura em busca de problemas de alto risco ou alto impacto relacionados à segurança, desempenho, custo e confiabilidade. Ele fornece informações detalhadas sobre os recursos afetados e as recomendações de remediação. Para obter uma lista completa de verificações e descrições, consulte a referência de AWS Trusted Advisor cheques (Trusted Advisor documentação).

Analise Trusted Advisor as descobertas de forma recorrente e corrija os problemas conforme necessário. Se você tiver os planos AWS Business Support ou Enterprise Support, poderá assinar um e-mail semanal de descobertas. Para obter mais informações, consulte Configurar preferências de notificação (documentação do AWS Support).

Para visualizar problemas em Trusted Advisor

- Revise cada categoria de verificação de acordo com as instruções em Exibir categorias de verificação (AWS Support documentação). No mínimo, recomendamos revisar os problemas de ação recomendada, marcados em vermelhao.

Como proteger suas workloads

Os controles e recomendações nesta seção ajudam você a proteger suas workloads em execução naAWS enquanto você as constrói. Eles enfatizam práticas seguras para gerenciar segredos e escopo de acesso de aplicações, minimizar as rotas de acesso a recursos privados e usar criptografia para proteger dados em trânsito e em repouso.

Esta seção contém os seguintes tópicos:

WKLD.01: usar perfis do IAM para permissões do ambiente computacional

No AWS Identity and Access Management (IAM), um perfil representa um conjunto de permissões que podem ser assumidas por uma pessoa ou serviço por um período de tempo configurável. O uso de perfis elimina a necessidade de armazenar ou gerenciar credenciais de longo prazo, reduzindo significativamente a chance de uso não intencional. Atribua um perfil do IAM diretamente

às instâncias do Amazon Elastic Compute Cloud (Amazon EC2), tarefas e serviços do AWS Fargate, funções do AWS Lambda e outros serviços de computação da AWS sempre que houver suporte. Aplicações que usam AWS SDK e são executados nesses ambientes computacionais usam automaticamente as credenciais do perfil do IAM para autenticação.

A abordagem e as instruções para usar os perfis do IAM para cada serviço podem ser encontradas na Documentação da AWS para o serviço. Por exemplo, consulte:

- Perfis do IAM para Amazon EC2 (documentação do Amazon EC2)
- Perfis do IAM para tarefas (documentação do Amazon Elastic Container Service)
- Perfil de execução do Lambda (documentação do Lambda)

WKLD.02: restringir o escopo de uso de credenciais com permissões de políticas baseadas em recursos

Políticas são objetos que podem definir permissões ou especificar condições de acesso. Existem dois tipos principais de políticas:

- Políticas baseadas em identidade são vinculadas a entidades principais e definem quais são as permissões da entidade principal no ambiente da AWS.
- Políticas baseadas em recursos são vinculadas a um recurso, como um bucket do Amazon Simple Storage Service (Amazon S3) ou endpoint de nuvem privada virtual (VPC). Essas políticas especificam quais entidades principais têm acesso permitido, ações válidas e quaisquer outras condições que devem ser atendidas.

Para que uma entidade principal tenha acesso para realizar uma ação contra um recurso, ela deve ter permissão concedida em sua política baseada em identidade e atender às condições da política baseada em recurso. Para obter mais informações, consulte Políticas baseadas em identidade e políticas baseadas em recursos (documentação do IAM).

As condições recomendadas para políticas baseadas em recursos incluem:

- Restrinja o acesso somente às entidades principais uma organização especificada (definida em AWS Organizations) usando a condição `aws:PrincipalOrgID`.
- Restrinja o acesso ao tráfego proveniente de uma VPC específica ou endpoint da VPC usando a condição `aws:SourceVpc` ou `aws:SourceVpce`, respectivamente.

- Permita ou negue o tráfego com base no endereço IP de origem usando uma condição `aws:SourceIp`.

O seguinte exemplo mostra uma política baseada em recursos que usa a condição `aws:PrincipalOrgID` para permitir entidades principais na organização **<o-xxxxxxxxxxx>** para acessar o bucket **<bucket-name>** do S3.

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
       "Effect":"Allow",
       "Principal":"*",
       "Action":"s3:*",
       "Resource":"arn:aws:s3:::<bucket-name>/*",
       "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
       }
     }
   ]
}
```

WKLD.03: usar segredos efêmeros ou um serviço de gerenciamento de segredos

Os segredos de aplicações consistem principalmente em credenciais, como pares de chaves, tokens de acesso, certificados digitais e credenciais de login. A aplicação usa esses segredos para obter acesso a outros serviços dos quais depende, como um banco de dados. Para ajudar a proteger esses segredos, recomendamos que eles sejam efêmeros (gerados no momento da solicitação e de curta duração, assim como os perfis do IAM) ou recuperados de um serviço de gerenciamento de segredos. Isso evita a exposição acidental por meio de mecanismos menos seguros, como a persistência em arquivos de configuração estáticos. E também facilita promover o código da aplicação desde os ambientes de desenvolvimento até os de produção.

Para um serviço de gerenciamento de segredos, recomendamos usar uma combinação do Parameter Store, um recurso do AWS Systems Manager, e o AWS Secrets Manager:

- Use o Parameter Store para gerenciar segredos e outros parâmetros que são pares individuais de chave-valor baseados em strings de tamanho geral curto e acessados com frequência. Use uma chave do AWS Key Management Service (AWS KMS) para criptografar o segredo. Não há cobrança para armazenar parâmetros no nível padrão do Parameter Store. Para obter mais informações sobre níveis de parâmetros, consulte Gerenciamento de níveis de parâmetros (documentação do Systems Manager).
- Use o Secrets Manager para armazenar segredos que estão em formato de documento (como vários pares de chave-valor relacionados), são maiores que 4 KB (como certificados digitais) ou que se beneficiariam da rotação automática.

É possível usar as APIs do Parameter Store para recuperar segredos armazenados no Secrets Manager. Isso permite padronizar o código em sua aplicação ao usar uma combinação dos dois serviços.

Para gerenciar segredos no Parameter Store

1. Criar uma chave do AWS KMS simétrica (documentação do AWS KMS).
2. Criar um parâmetro SecureString (documentação do Systems Manager). Os segredos no Parameter Store usam o tipo de dados `SecureString`.
3. Na aplicação, recupere um parâmetro do Parameter Store usando o AWSSDK para sua linguagem de programação. Para obter um exemplo em Java, consulte GetParameter.java (Catálogo de exemplos de código da AWS).

Para gerenciar no Secrets Manager

1. Criar um segredo (documentação do Secrets Manager).
2. Recuperar segredos do AWS Secrets Manager no código (documentação do Secrets Manager).

   É importante ler Use bibliotecas de cache do lado do cliente do AWS Secrets Manager para melhorar a disponibilidade e a latência do uso de seus segredos (publicação no blog da AWS). O uso de SDKs no lado do cliente, que já têm as práticas recomendadas implementadas, deve acelerar e simplificar o uso e a integração do Secrets Manager.

WKLD.04: impedir que segredos de aplicações sejam expostos

Durante o desenvolvimento local, os segredos de uma aplicação podem ser armazenados na configuração local ou em arquivos de código e inseridos acidentalmente nos repositórios de código-fonte. Repositórios não seguros hospedados em provedores de serviços públicos podem estar sujeitos ao acesso não autorizado e à descoberta subsequente desses segredos. Use as ferramentas disponíveis para evitar o check-in de segredos. Incorpore verificações de segredos expostos como parte de seus processos manuais de revisão de código.

Algumas ferramentas comuns que podem impedir que segredos de aplicações sejam registrados nos repositórios de código-fonte são:

- Gitleaks (repositório GitHub)
- Whispers (repositório GitHub)
- detect-secrets (repositório GitHub)
- git-secrets (repositório GitHub)
- TruffleHog (repositório GitHub)

WKLD.05: detectar e corrigir segredos expostos

Em WKLD.03: usar segredos efêmeros ou um serviço de gerenciamento de segredos e WKLD.04: impedir que segredos de aplicações sejam expostos, você implementou medidas para proteger segredos. Neste controle, você implanta uma solução que pode detectar se os segredos contornaram essas medidas de prevenção e pode corrigir o problema da forma adequada.

O Amazon CodeGuru Reviewer detecta segredos de aplicações no código-fonte e fornece um mecanismo para corrigir e publicar os segredos detectados no Secrets Manager. O código da aplicação para recuperar o segredo do Secrets Manager também é fornecido. Faça uma análise de custo-benefício para determinar se essa solução é adequada para sua empresa. Como alternativa, algumas das soluções de código aberto em WKLD.04: impedir que segredos de aplicações sejam expostos oferecem capacidade de detecção de segredos existentes.

Para configurar a integração do CodeGuru Reviewer com o Secrets Manager

- Use o CodeGuru Reviewer para identificar segredos codificados e o AWS Secrets Manager para protegê-los (postaegm no blog da AWS e passo a passo guiado).

WKLD.06: usar o Systems Manager em vez de SSH ou RDP

Sub-redes públicas, aquelas que têm uma rota padrão apontando para um gateway da Internet, são inerentemente um risco de segurança maior do que as sub-redes privadas, as sem rota para a Internet. É possível executar instâncias do EC2 em sub-redes privadas e usar o recurso Gerenciador de Sessões do AWS Systems Manager para acessar remotamente as instâncias por meio da AWS Command Line Interface (AWS CLI) ou do AWS Management Console. Em seguida, você pode usar a AWS CLI ou o console para iniciar uma sessão que se conecta à instância por meio de um túnel seguro, evitando a necessidade de gerenciar credenciais adicionais usadas para o Secure Shell (SSH) ou o protocolo de desktop remoto (RDP) do Windows.

Use o Gerenciador de Sessões em vez de executar instâncias do EC2 em sub-redes públicas, executar jump boxes ou executar bastion hosts.

Para configurar o Session Manager

1. Certifique-se de que a instância do EC2 esteja usando as imagens de máquina da Amazon (AMIs) do sistema operacional mais recente, como Amazon Linux 2 ou Ubuntu. O AWS Systems Manager Agent (SSM Agent) é pré-instalado na AMI.
2. Certifique-se de que a instância tenha conectividade, seja por meio de um gateway da Internet ou via endpoints da VPC, com esses endereços (substituindo **`<region>`** pela Região da AWS apropriada):
    a. Ec2messages.<region>.amazonaws.com
    b. ssm.<region>.amazonaws.com
    c. ssmmessages.<region>.amazonaws.com
3. Anexe a política gerenciada pela AWS `AmazonSSMManagedInstanceCore` ao perfil do IAM associado às suas instâncias.

Para obter mais informações, consulte Configurar o Session Manager (documentação do Systems Manager).

Para iniciar uma sessão

- Iniciar uma sessão (documentação do Systems Manager).

WKLD.07: registrar eventos de dados para buckets do S3 com dados confidenciais

Por padrão, o AWS CloudTrail captura eventos de gerenciamento, eventos que criam, modificam ou excluem recursos em sua conta. Esses eventos de gerenciamento não capturam operações de leitura ou gravação em objetos individuais nos buckets do Amazon Simple Storage Service. Durante um evento de segurança, é importante capturar o acesso ou o uso não autorizado de dados em nível de objeto ou registro individual. Use o CloudTrail para registrar eventos de dados para qualquer bucket do S3 que armazene dados confidenciais ou essenciais aos negócios para fins de detecção e auditoria.

> **Note**
>
> Há cobranças adicionais para o registro de eventos de dados. Para obter mais informações, consulte Preço do AWS CloudTrail.

Para registrar em log eventos de dados para trilhas

1. Faça login no AWS Management Console e abra o console do CloudTrail em https://console.aws.amazon.com/cloudtrail/
2. No painel de navegação, escolha Trilhas e o nome da trilha.
3. Em Detalhes gerais, escolha Editar para alterar as configurações a seguir. Não é possível alterar o nome de uma trilha.
    a. Em Eventos de dados, escolha Editar.
    b. Em Data event source (Fonte do eventos de dados), escolha S3.
    c. Em Todos os buckets S3 atuais e futuros, desmarque Leitura e Gravação.
    d. Em Seleção de bucket individual, procure pelo bucket no qual registrar eventos de dados. É possível selecionar vários buckets nesta janela. Escolha Add bucket (Adicionar bucket) para registrar eventos de dados em mais buckets. Escolha se você deseja registrar eventos de Read (Leitura), como `GetObject`, Write (Gravação), como `PutObject`, ou ambos.
    e. Escolha Update Trail (Atualizar trilha).

WLD.08: criptografar volumes do Amazon EBS

Imponha a criptografia dos volumes do Amazon Elastic Block Store (Amazon EBS) como o comportamento padrão em sua conta da AWS. Os volumes criptografados apresentam a mesma performance de operações de entrada e saída por segundo (IOPS) que os volumes não criptografados, com um efeito mínimo na latência. Isso evita a reconstrução de volumes em uma data posterior por motivos de conformidade ou outros. Para obter mais informações, consulte As práticas recomendadas que você precisa conhecer para a criptografia do Amazon EBS (publicação no blog da AWS).

Para criptografar volumes do Amazon EBS

- Habilitar a criptografia por padrão (documentação do Amazon EC2).

WKLD.09: criptografar bancos de dados do Amazon RDS

De forma semelhante a WLD.08: criptografar volumes do Amazon EBS, habilite a criptografia dos bancos de dados do Amazon Relational Database Service (Amazon RDS). Essa criptografia é executada no nível do volume subjacente e apresenta a mesma performance de IOPS que os volumes não criptografados, com um efeito mínimo na latência. Para obter mais informações, consulte Visão geral da criptografia de recursos do Amazon RDS (documentação do Amazon RDS).

Para criptografar uma instância de banco de dados do RDS

- Criptografar uma instância de banco de dados (documentação do Amazon RDS).

WKLD.10: implantar recursos privados em sub-redes privadas

Implante recursos que não exijam acesso direto à Internet, como instâncias do EC2, bancos de dados, filas, armazenamento em cache ou outra infraestrutura, em uma sub-rede privada da VPC. As sub-redes privadas não têm uma rota declarada em sua tabela de rotas para um gateway da Internet conectado e não podem receber tráfego da Internet. O tráfego proveniente de uma sub-rede privada destinado à Internet deve passar pela conversão de endereços de rede (NAT) por meio de um sistema AWS NAT Gateway gerenciado ou uma instância do EC2 que executa processos de NAT em uma sub-rede pública. Para obter mais informações sobre isolamento de redes, consulte Segurança da infraestrutura na Amazon VPC (documentação da Amazon VPC).

Use as seguintes práticas ao criar recursos e sub-redes privadas:

- Ao criar uma sub-rede privada, desabilite Atribuir endereço IPv4 público automaticamente.
- Ao criar instâncias do EC2 privadas, desabilite Atribuir IP público automaticamente. Isso evita que um IP público seja atribuído se a instância for implantada acidentalmente em uma sub-rede pública em função de uma configuração incorreta.

Quando necessário, especifique a sub-rede de um recurso como parte de sua configuração. É possível implantar uma VPC que atenda às práticas recomendadas usando o Início rápido da arquitetura VPC modular e escalável (Inícios rápidos da AWS).

WKLD.11: restringir o acesso à rede usando grupos de segurança

Use grupos de segurança para controlar o tráfego para instâncias do EC2, bancos de dados do RDS e outros recursos compatíveis. Os grupos de segurança atuam como um firewall virtual que pode ser aplicado a qualquer grupo de recursos relacionados para definir consistentemente regras para permitir tráfego de entrada e saída. Além das regras baseadas em endereços IP e portas, os grupos de segurança oferecem suporte a regras para permitir o tráfego de recursos associados a outros grupos de segurança. Por exemplo, um grupo de segurança de banco de dados pode ter regras para permitir somente o tráfego de um grupo de segurança do servidor de aplicações.

Por padrão, os grupos de segurança permitem todo o tráfego de saída, mas não permitem o tráfego de entrada. A regra de tráfego de saída pode ser removida ou você pode configurar regras adicionais para restringir o tráfego de saída e permitir o tráfego de entrada. Se o grupo de segurança não tiver nenhuma regra de saída, nenhum tráfego de saída proveniente da instância será permitido. Para obter mais informações, consulte Controlar o tráfego para recursos usando grupos de segurança (documentação da Amazon VPC).

No exemplo a seguir, há três grupos de segurança que controlam o tráfego de um Application Load Balancer para instâncias do EC2 que se conectam a um banco de dados do Amazon RDS para MySQL.

Grupo de segurança	Regras de entrada	Regras de saída
Grupo de segurança do Application Load Balancer	Descrição: permitir tráfego HTTPS de qualquer lugar Tipo: HTTPS	Descrição: permitir todo o tráfego para qualquer lugar Tipo: todo o tráfego

Grupo de segurança	Regras de entrada	Regras de saída
	Origem: Anywhere-IPv4 (0,0.0.0/0)	Destino: Anywhere-IPv4 (0,0.0.0/0)
Grupo de segurança da instância do EC2	Descrição: permitir tráfego HTTP do Application Load Balancer Tipo: HTTP Origem: grupo de segurança do Application Load Balancer	Descrição: permitir todo o tráfego para qualquer lugar Tipo: todo o tráfego Destino: Anywhere-IPv4 (0,0.0.0/0)
Grupo de segurança do banco de dados do RDS	Descrição: permitir tráfego MySQL proveniente da instância do EC2 Tipo:MySQL Origem: grupo de segurança da instância do EC2	Sem regras de saída

WKLD.12: usar endpoints da VPC para acessar serviços compatíveis

Nas VPCs, os recursos que precisam acessar a AWS ou outros serviços externos exigem uma rota para a Internet (`0.0.0.0/0`) ou para o endereço IP público do serviço de destino. Use endpoints da VPC para habilitar uma rota IP privada da sua VPC para o serviço da AWS ou outros serviços compatíveis, evitando assim a necessidade de usar um gateway da Internet, dispositivo NAT, conexão de rede virtual privada (VPN) ou conexão do AWS Direct Connect.

Os endpoints da VPC oferecem suporte à anexação de políticas e grupos de segurança para controlar ainda mais o acesso a um serviço. Por exemplo, você pode escrever uma política de endpoint da VPC para o Amazon DynamoDB para permitir somente ações em nível de item e evitar ações em nível de tabela para todos os recursos na VPC, independentemente de sua própria política de permissão. Você também pode criar uma política de bucket do S3 para permitir somente solicitações provenientes de um endpoint da VPC específico, negando todos os outros acessos

externos. Um endpoint da VPC também pode ter uma regra de grupo de segurança que, por exemplo, restringe o acesso somente a instâncias do EC2 associadas a um grupo de segurança específico da aplicação, como a camada de lógica de negócios de uma aplicação Web.

Existem diferentes tipos de endpoints da VPC. Você acessa a maioria dos serviços usando um endpoint de interface da VPC. O DynamoDB é acessado por meio de um endpoint de gateway. O Amazon S3 oferece suporte a endpoints de interface e de gateway. Os endpoints de gateway são recomendados para workloads contidas em uma única conta e região da AWS, sem custo adicional. Os endpoints de interface são recomendados em caso de necessidade de um acesso mais extensível, como a um bucket do S3 de outras VPCs, de redes on-premises ou de diferentes Regiões da AWS. Os endpoints de interface incorrem em uma taxa de disponibilidade por hora e uma taxa de processamento de dados por GB, ambas inferiores às respectivas cobranças pelo envio dos dados para `0.0.0.0/0` via AWS NAT Gateway.

Para obter mais informações sobre o uso de endpoints da VPC, consulte os seguintes recursos adicionais:

- Para obter mais informações sobre como selecionar entre endpoints de gateway e interface para o Amazon S3, consulte Como escolher sua estratégia de endpoint da VPC para o Amazon S3 (publicação no blog da AWS).
- Criar um endpoint de interface (documentação da Amazon VPC).
- Criar um endpoint de gateway (documentação da Amazon VPC).
- Para obter exemplos de políticas de bucket do S3 que restringem o acesso a uma VPC ou endpoint da VPC específico, consulte Como restringir o acesso a uma VPC específica (documentação do Amazon S3).
- Para obter exemplos de políticas de endpoint do DynamoDB que restringem ações, consulte Políticas de endpoint para o DynamoDB (documentação da Amazon VPC).

WKLD.13: exigir HTTPS para todos os endpoints da Web públicos

Exija HTTPS para fornecer credibilidade adicional aos seus endpoints da Web, permita que os endpoints usem certificados para provar sua identidade e confirme se todo o tráfego entre seu endpoint e os clientes conectados está criptografado. Para sites públicos, isso oferece o benefício adicional de uma classificação mais alta nos mecanismos de pesquisa.

Muitos serviços da AWS fornecem endpoints públicos da Web para seus recursos, como o AWS Elastic Beanstalk, Amazon CloudFront, Amazon API Gateway, Elastic Load Balancing e AWS Amplify. Para obter instruções sobre como exigir HTTPS para cada um desses serviços, consulte:

- Elastic Beanstalk (documentação do Elastic Beanstalk)
- CloudFront (documentação do CloudFront)
- Application Load Balancer (Centro de Conhecimentos da AWS)
- Classic Load Balancer (Centro de Conhecimentos da AWS)
- Amplify (documentação do Amplify)

Os sites estáticos hospedados no Amazon S3 não oferecem suporte a HTTPS. Para exigir HTTPS para esses sites, é possível usar o CloudFront. Não é necessário acesso público aos buckets do S3 que estão servindo conteúdo por meio do CloudFront.

Para usar o CloudFront para servir um site estático hospedado no Amazon S3

1. Usar o CloudFront para servir um site estático hospedado no Amazon S3 (Centro de Conhecimentos da AWS).
2. Se você estiver configurando o acesso a um bucket público do S3, exija HTTPS entre os visualizadores e o CloudFront (documentação do CloudFront).

   Se você estiver configurando o acesso a um bucket do S3 privado, restrinja o acesso ao conteúdo do Amazon S3 usando uma identidade de acesso de origem (documentação do CloudFront).

Além disso, configure endpoints HTTPS para exigir protocolos e cifras modernos de Transport Layer Security (TLS), a menos que a compatibilidade com protocolos mais antigos seja necessária. Por exemplo, use `ELBSecurityPolicy-FS-1-2-Res-2020-10` ou a política mais recente disponível para receptores HTTPS do Application Load Balancer, em vez da `ELBSecurityPolicy-2016-08` padrão. As políticas mais atuais exigem no mínimo TLS 1.2, sigilo de encaminhamento e cifras fortes que sejam compatíveis com navegadores da Web modernos.

Para obter mais informações sobre as políticas de segurança disponíveis para endpoints públicos HTTPS, consulte:

- Políticas de segurança SSL predefinidas para Classic Load Balancers (documentação do Elastic Load Balancing)

- Políticas de segurança para seu Application Load Balancer (documentação do Elastic Load Balancing)
- Protocolos e cifras compatíveis entre visualizadores e o CloudFront (documentação do CloudFront)

WKLD.14: usar serviços de proteção de borda para endpoints públicos

Em vez de fornecer tráfego diretamente de serviços computacionais, como instâncias do EC2 ou contêineres, use um serviço de proteção de borda. Isso fornece uma camada adicional de segurança entre o tráfego de entrada da Internet e seus recursos que atendem a esse tráfego. Esses serviços podem filtrar tráfego indesejado, aplicar criptografia e aplicar regras de roteamento ou outras regras, como balanceamento de carga, antes que o tráfego chegue aos seus recursos internos.

Os serviços da AWS que podem fornecer proteção pública de endpoints incluem o AWS WAF, CloudFront, Elastic Load Balancing, API Gateway e Amplify Hosting. Execute serviços baseados em VPC, como o Elastic Load Balancing, em uma sub-rede pública como um proxy para recursos de serviços Web executados em uma sub-rede privada.

O CloudFront, o API Gateway e o Amazon Route 53 oferecem proteção contra ataques distribuídos de negação de serviço (DDoS) das camadas 3 e 4 sem nenhum custo, e o AWS WAF pode proteger contra ataques de camada 7.

As instruções para começar a usar cada um desses serviços podem ser encontradas aqui:

- Conceitos básicos do AWS WAF (site do AWS)
- Conceitos básicos do Amazon CloudFront (documentação do CloudFront)
- Conceitos básicos do Elastic Load Balancing (documentação do Elastic Load Balancing)
- Conceitos básicos do API Gateway (documentação do API Gateway)
- Conceitos básicos do Amplify Hosting (documentação do Amplify)

WKLD.15: definir controles de segurança em modelos e implantá-los usando práticas de CI/CD

Infrastructure como código (IaC) é a prática de definir todos os seus recursos de serviços da AWS e configurações em modelos e códigos que você implanta usando pipelines de integração contínua e

entrega contínua (CI/CD), os mesmos pipelines usados para implantar aplicações de software. Os serviços de IaC, como o AWS CloudFormation, são compatíveis com políticas baseadas em recursos e em identidades do IAM e oferecem suporte a serviços de segurança da AWS, como o Amazon GuardDuty, AWS WAF e Amazon VPC. Capture esses artefatos como modelos de IaC, confirme os modelos em um repositório de código-fonte e, em seguida, implante-os usando pipelines de CI/CD.

A menos que seja exigido de outra forma, confirme as políticas de permissão da aplicação com o código da aplicação no mesmo repositório e gerencie as políticas gerais de recursos e as configurações do serviço de segurança em repositórios de código e pipelines de implantação separados.

Para obter mais informações sobre como começar a usar IaC na AWS, consulte a documentação do AWS Cloud Development Kit (AWS CDK).

Contribuidores

Os colaboradores deste documento incluem:

- Jay Michael, arquiteto principal de soluções
- Cole Calistra, arquiteto principal de soluções
- Justin Plock, arquiteto principal de soluções
- Faisal Farooq, arquiteto de soluções
- Michael Nguyen, arquiteto sênior de soluções
- Ritik Khatwani, arquiteto sênior de soluções
- Paul Hawkins, diretor, diretor de segurança da informação (CISO)

Um agradecimento especial às seguintes pessoas que também ajudaram com orientação e revisão:

- Robert Put
- Mike Sullivan
- Bob Lee III

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
Configurações do bucket do Amazon S3	Atualizamos a seção ACCT.08: impedir o acesso público a buckets do S3 privados para refletir que os buckets do Amazon S3 criados após 28 de abril de 2023 têm a configuração Bloquear acesso público habilitada por padrão.	18 de maio de 2023
Práticas recomendadas de segurança do IAM	Atualizamos este guia para alinhamento com as mais recentes práticas recomendadas do AWS Identity and Access Management (IAM). Para obter mais informações, consulte Práticas recomendadas de segurança na documentação do IAM.	1 de fevereiro de 2023
Perfis do IAM	Fornecemos links adicionais para a documentação do AWS service (Serviço da AWS) na seção WKLD.01: usar perfis do IAM para permissões do ambiente computacional.	22 de setembro de 2022
Política de senhas	Atualizamos as recomendações de senhas fortes para usar as orientações mais	10 de maio de 2022

	recentes do Center for Internet Security (CIS).	
Publicação inicial	—	13 de abril de 2022

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Aurora Edição Compatível com PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: migre seu banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) para Oracle na nuvem. AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migrar seu sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: migre seu banco de dados Oracle local para o Oracle em uma instância do EC2 na nuvem. AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Esse cenário de migração é específico do VMware Cloud on AWS, que oferece suporte à compatibilidade de máquinas virtuais (VM) e à portabilidade da carga de trabalho entre seu ambiente local e. AWSÉ 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 on. 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 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 AWS na documentação AWS Identity and Access Management (IAM).

fonte de dados autorizada

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

Availability Zone (zona de disponibilidade)

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o site da AWS CAF e o whitepaper da AWS CAF.

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

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

B

bot ruim

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

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

acesso em vidro quebrado

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

planejamento de continuidade de negócios (BCP)

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

C

CAF

Consulte Estrutura de adoção da AWS nuvem.

implantação canária

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

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja a integração e a entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de Excelência 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 postagens do CCoE no blog AWS Cloud Enterprise Strategy.

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam quando migram para a AWS nuvem:

- 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 postagem do blog The Journey Toward Cloud-First & the Stages of Adoption no blog AWS Cloud Enterprise Strategy. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

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

desvio de dados

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

dados em trânsito

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

malha de dados

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta é chamada de administrador delegado para esse serviço Para obter mais informações e uma

lista de serviços compatíveis, consulte Serviços que funcionam com o AWS Organizations na documentação do AWS Organizations .

implantação

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

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

recuperação de desastres (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 de cargas de trabalho em AWS: Recuperação na nuvem no AWS Well-Architected Framework.

DML

Consulte linguagem de manipulação de banco de dados.

design orientado por domínio

Uma abordagem ao desenvolvimento de um sistema de software complexo conectando seus componentes aos domínios em evolução, ou principais metas de negócios, atendidos por cada componente. Esse conceito foi introduzido por Eric Evans em seu livro, Design orientado por domínio: lidando com a complexidade no coração do software (Boston: Addison-Wesley Professional, 2003). Para obter informações sobre como 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. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros diretores Contas da AWS ou a AWS Identity and Access Management (IAM). Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais informações, consulte Criar um serviço de endpoint na documentação do Amazon Virtual Private Cloud (Amazon VPC).

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

environment (ambiente)

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

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

epic

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

ERP

Consulte planejamento de recursos corporativos.

análise exploratória de dados (EDA)

O processo de analisar um conjunto de dados para entender suas principais características. Você coleta ou agrega dados e, em seguida, realiza investigações iniciais para encontrar padrões,

detectar anomalias e verificar suposições. 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 operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: aquelas que contêm medidas e aquelas que contêm uma chave externa para uma tabela de dimensões.

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a filial.

recursos

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

importância do recurso

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

transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo,

se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

FGAC

Veja o controle de acesso refinado.

controle de acesso refinado (FGAC)

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

migração flash-cut

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

G

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

estratégia greenfield

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

barreira de proteção

Uma regra de alto nível que ajuda a 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 usando AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

migração homogênea de bancos de dados

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

para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

dados quentes

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

hotfix

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

período de hipercuidados

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

I

IaC

Veja a infraestrutura como código.

Política baseada em identidade

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

aplicação ociosa

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

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 AWS várias contas, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de um aplicativo. 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.

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet 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 AWS várias contas, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (na mesma ou em diferentes Regiões da AWS), a Internet e as redes locais. A Arquitetura de referência de 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 landing zone é um AWS ambiente bem arquitetado, com várias contas, escalável e seguro. Um ponto a partir do qual suas organizações podem iniciar e implantar rapidamente workloads e aplicações com confiança em seu ambiente de segurança e infraestrutura. Para obter mais informações sobre zonas de pouso, consulte Configurar um ambiente da AWS com várias contas seguro e escalável.

migração de grande porte

: Uma migração de 300 servidores ou mais.

LBAC

: Veja controle de acesso baseado em etiquetas.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

: Veja 7 Rs.

sistema little-endian

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

ambientes inferiores

: Veja o ambiente.

M

machine learning (ML)

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

ramificação principal

Veja a filial.

malware

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

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

conta-membro

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

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens (MQTT)

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

microsserviço

Um serviço pequeno e independente que se comunica 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 Integração de microsserviços usando serviços sem AWS servidor.

arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio de uma interface bem definida usando 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 Implementação de microsserviços em. AWS

Programa de Aceleração da Migração (MAP)

Um AWS programa que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a compensar o custo inicial das migrações. O MAP inclui uma metodologia de migração para executar migrações legadas de forma metódica e um conjunto de ferramentas para automatizar e acelerar cenários comuns de migração.

migração em escala

O processo de mover a maior parte do portfólio de aplicações para a nuvem em ondas, com mais aplicações sendo movidas em um ritmo mais rápido a cada onda. Essa fase usa as práticas

recomendadas e lições aprendidas nas fases anteriores para implementar uma fábrica de migração de equipes, ferramentas e processos para agilizar a migração de workloads por meio de automação e entrega ágeis. Esta é a terceira fase da estratégia de migração para a AWS.

fábrica de migração

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

metadados de migração

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

padrão de migração

Uma tarefa de migração repetível que detalha a estratégia de migração, o destino da migração e a aplicação ou o serviço de migração usado. Exemplo: rehospede a migração para o Amazon EC2 AWS com o Application Migration Service.

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja o aprendizado de máquina.

modernização

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

avaliação de preparação para modernização

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

MAPA

Consulte Avaliação do portfólio de migração.

MQTT

Consulte Transporte de telemetria de enfileiramento de mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja o controle de acesso de origem.

CARVALHO

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

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

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

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

OPC-UA

Consulte Comunicação de processo aberto — Arquitetura unificada.

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

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (OT)

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

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

Uma estrutura para gerenciar grandes transformações de negócios disruptivas de uma perspectiva de pessoas, cultura e liderança. O OCM ajuda as organizações a se prepararem

e fazerem a transição para novos sistemas e estratégias, acelerando a adoção de alterações, abordando questões de transição e promovendo mudanças culturais e organizacionais. Na estratégia de AWS migração, essa estrutura é chamada de aceleração de pessoas, devido à velocidade de mudança necessária nos projetos de adoção da nuvem. Para obter mais informações, consulte o guia do OCM.

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

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

OU

Veja a análise de prontidão operacional.

NÃO

Veja a tecnologia operacional.

VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A Arquitetura de referência de 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.

PLC

Consulte controlador lógico programável.

AMEIXA

Veja o gerenciamento do ciclo de vida do produto.

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pressão de predicados

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

controle preventivo

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

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais informações, consulte Entidade principal em Termos e conceitos de perfis na documentação do IAM.

Privacidade por design

Uma abordagem 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.

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja o ambiente.

controlador lógico programável (PLC)

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

pseudonimização

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

publicar/assinar (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

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

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)

Período de tempo aceitável máximo desde o último ponto de recuperação de dados. 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 AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter mais informações, consulte Especificar o que Regiões da AWS sua conta pode usar.

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

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 o login único federado (SSO), para que os usuários possam fazer login AWS Management Console ou chamar as operações da AWS API sem que você precise criar um usuário no IAM para todos

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

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

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

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

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização 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 serviço na AWS Organizations documentação.

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

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

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

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

CUSPE

Veja um único ponto de falha.

esquema de estrelas

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

padrão strangler fig

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

sub-rede

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

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o ambiente.

treinamento

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

gateway de trânsito

Um hub de trânsito de rede que 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 AWS Transit Gateway documentação.

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o ambiente.

V

aspiração

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

controle de versões

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

emparelhamento 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.