



Transição para vários Contas da AWS

AWS Orientação prescritiva



AWS Orientação prescritiva: Transição para vários Contas da AWS

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Introdução	1
Público-alvo	2
Resultados de negócios direcionados	3
Exemplo de arquitetura de conta única	3
Estrutura fundamental	5
AWS Well-Architected Framework	5
Base na nuvem na AWS	5
Gerenciamento de identidade e controle de acesso	6
Configurar uma organização	6
Práticas recomendadas	7
Criar uma zona de pouso	8
Práticas recomendadas	8
Adicionar unidades organizacionais	9
Práticas recomendadas	10
Adicionar usuários iniciais	10
Práticas recomendadas	11
Gerenciar contas-membro	12
Convidar sua conta pré-existente	12
Personalizar as configurações da VPC no AWS Control Tower	14
Definir os critérios de escopo	15
Gerenciar permissões e acesso	17
Considerações culturais de engenharia	17
Criar conjuntos de permissões	18
Conjunto de permissões de faturamento	18
Conjunto de permissões de desenvolvedor	19
Conjunto de permissões de produção	21
Criar um limite de permissões	22
Gerenciar permissões para indivíduos	25
Conectividade de rede	27
Conectar VPCs	27
Conectar aplicações	27
Práticas recomendadas	28
Saída centralizada	28
Práticas recomendadas para proteger o tráfego de saída	30

Entrada descentralizada	31
Resposta a um incidente de segurança	34
Amazon GuardDuty	34
Práticas recomendadas	35
Amazon Macie	35
Práticas recomendadas	36
AWS Security Hub	36
Práticas recomendadas	37
Backups	38
Migração de contas	39
Migração de recursos	41
AWS AppConfig	42
AWS Certificate Manager	42
Amazon CloudFront	42
AWS CodeArtifact	42
Amazon DynamoDB	43
Amazon EBS	43
Amazon EC2	43
Amazon ECR	44
Amazon EFS	44
Amazon ElastiCache (RedisOSS)	44
AWS Elastic Beanstalk	44
Endereços IP elásticos	45
AWS Lambda	45
Amazon Lightsail	45
Amazon Neptune	45
OpenSearch Serviço Amazon	46
Amazon RDS	46
Amazon Redshift	46
Amazon Route 53	46
Amazon S3	47
Amazon SageMaker	47
AWS WAF	47
Considerações sobre faturamento	49
Conclusão	50
Colaboradores	51

Recursos	52
Recomendações da AWS	52
Publicações no blog da AWS	52
Whitepapers da AWS	52
Exemplos de código da AWS	52
Histórico do documento	53
Glossário	55
#	55
A	56
B	59
C	61
D	64
E	68
F	70
G	72
H	72
I	74
L	76
M	77
O	81
P	84
Q	87
R	87
S	90
T	94
U	95
V	96
W	96
Z	97
.....	xcviii

Transição para várias Contas da AWS

Amazon Web Services ([colaboradores](#))

Maio de 2024 ([histórico do documento](#))

Muitas empresas começam sua jornada usando uma única conta do Amazon Web Services (AWS). Vários perfis em uma empresa usam essa conta para operar os negócios. Os engenheiros desenvolvem código, implantam em ambientes de desenvolvimento e teste e promovem mudanças na produção. Os gerentes de produto consultam fontes de dados para coletar insights sobre a performance dos negócios. A equipe de vendas está conduzindo demonstrações do ambiente de produção para atrair novos clientes. A equipe financeira está monitorando os gastos com a nuvem a partir do AWS Billing console.

Quando todas essas funções separadas usam uma única Conta da AWS, pode ser difícil aplicar a melhor prática de segurança de [aplicar as permissões de privilégio mínimo, o que significa que você concede somente as permissões](#) mínimas necessárias para realizar o trabalho. Em um determinado estágio do desenvolvimento de uma startup, alguém fará a pergunta Todos os nossos engenheiros precisam ter acesso à produção? A resposta é quase sempre não, mas muitas empresas têm dificuldade em transformar seu ambiente de conta única existente em um ambiente de várias contas sem desacelerar os negócios.

Este guia inclui práticas recomendadas para ajudar você a fazer a transição de um ambiente de conta única para um ambiente de várias contas. Ele discute as decisões que você precisa tomar sobre migração de contas, gerenciamento de usuários, rede, segurança e arquitetura. Ele foi projetado para ajudar você a ter sucesso com tempo de inatividade mínimo ou inexistente para seus negócios e operações diárias. Este guia se concentra nos seguintes recursos à medida que você faz a transição de um ambiente de uma única conta Conta da AWS para um ambiente com várias contas:

- [Gerenciamento de identidade e controle de acesso](#)
- [Gerenciar permissões e acesso](#)
- [Conectividade de rede](#)
- [Resposta a um incidente de segurança](#)
- [Backups](#)
- [Migração de contas](#)

- [Migração de recursos](#)
- [Considerações sobre faturamento](#)

Para obter mais informações sobre recursos, consulte [Base na nuvem na AWS](#).

Este guia está alinhado aos recursos existentes relacionados a esse tópico, incluindo a [AWS Startup Security Baseline](#) (AWS SSB), o whitepaper [Organizing Your AWS Environment Using Multiple Accounts](#), a [AWS Security Reference Architecture](#) (AWS SRA) e o whitepaper [Establishing Your Cloud Foundation on AWS](#). Você deve continuar usando esses recursos para obter orientações mais específicas não abordadas neste guia.

Público-alvo

Este guia é mais adequado para empresas que desejam ou precisam fazer a transição para várias Contas da AWS. Para startups, essa necessidade geralmente surge quando você encontra um produto adequado ao mercado, arrecada uma rodada de financiamento e começa a contratar disciplinas de engenharia distintas, como infraestrutura, operações de desenvolvimento (DevOps) ou segurança.

Mesmo que sua empresa não esteja pronta para fazer essa transição, você ainda poderá usar este guia para entender as decisões que precisam ser tomadas durante a transição e começar a se preparar.

Resultados comerciais direcionados para transição para uma arquitetura de várias contas

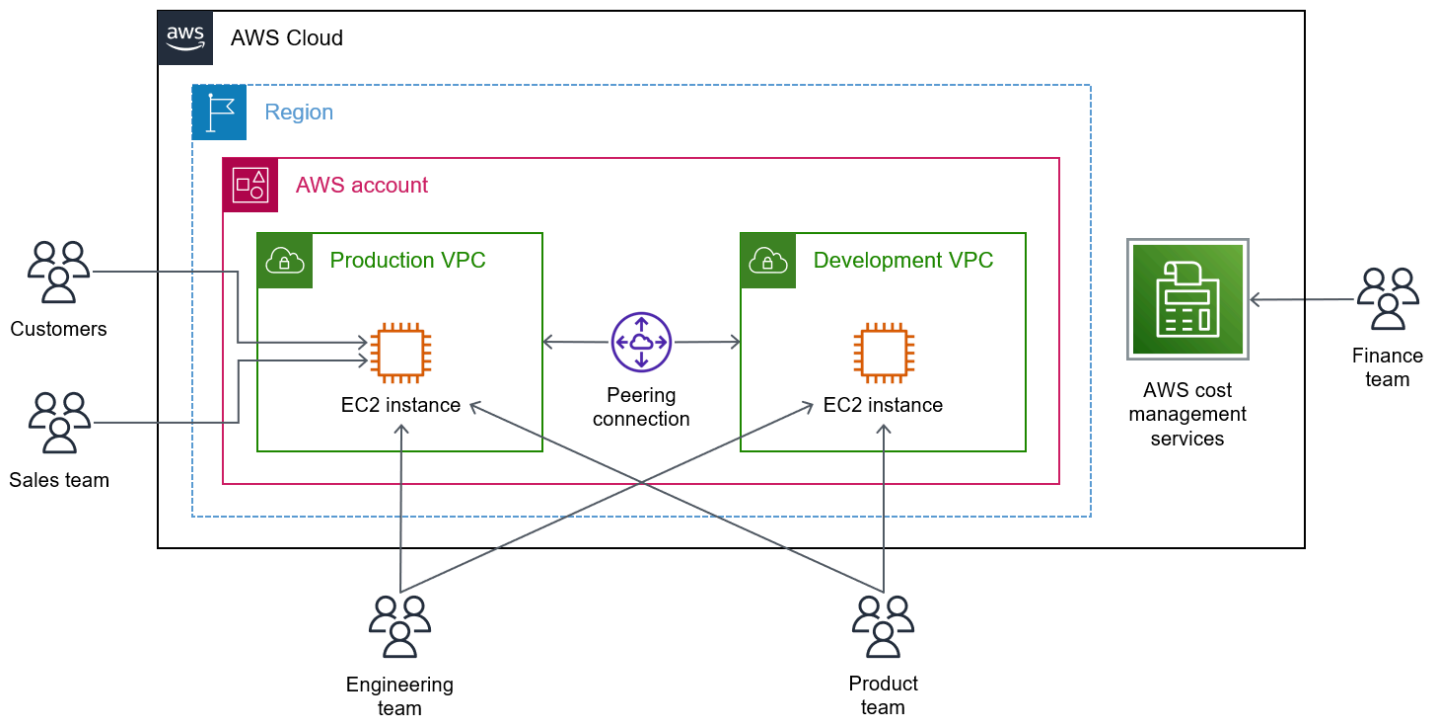
A transição para uma arquitetura de várias contas geralmente é impulsionada pela necessidade comercial de um ou mais dos seguintes benefícios:

- Agrupamento de workloads com base em objetivo comercial ou propriedade
- Aplicar controles de segurança distintos por ambiente
- Restringir o acesso a dados confidenciais
- Promover inovação e agilidade
- Limitar o escopo do impacto de eventos adversos
- Compatibilidade com vários modelos operacionais de TI
- Gerenciar custos
- Distribuir cotas do AWS service (Serviço da AWS) e limites de taxa de solicitação de API

Para obter mais informações sobre os vários benefícios de usar uma arquitetura de várias contas, consulte [Organizar seu ambiente da AWS usando várias contas](#) (whitepaper da AWS) e [Diretrizes para configurar um ambiente bem arquitetado](#) (documentação do AWS Control Tower).

Exemplo de arquitetura de conta única

Como ponto de partida, é comum que startups ou pequenas empresas usem uma única Região da AWS e tenham duas nuvens privadas virtuais (VPCs) conectadas por [Emparelhamento de VPC](#). Cada VPC contém recursos de computação, como instâncias do Amazon Elastic Compute Cloud (Amazon EC2). A equipe de engenharia desenvolve código diretamente na VPC de desenvolvimento. A equipe de produto revisa as alterações e, em seguida, a equipe de engenharia promove manualmente as alterações na VPC de produção. A equipe financeira tem acesso à Conta da AWS para que eles possam revisar o console do AWS Billing and Cost Management.



Veja a seguir alguns exemplos de desafios que uma empresa pode enfrentar com esse ambiente:

- Um engenheiro excluiu por engano os dados de produção quando pensou que estava acessando um banco de dados de desenvolvimento.
- Uma demonstração de vendas foi afetada quando uma implantação de produção demorou mais do que o esperado.
- Quando o código de desenvolvimento estava sendo testado em carga, a VPC de produção ficou lenta e gerou mensagens de erro sobre controle de utilização.
- A equipe financeira não consegue diferenciar os custos dos ambientes de produção e desenvolvimento.
- O CEO está preocupado com o fato de alguns empreiteiros offshore recém-contratados terem acesso aos dados do cliente por meio da VPC de produção.
- A equipe financeira não pode proibir acesso a Serviços da AWS específicos que podem incorrer em altos custos.

A adoção de uma estratégia de várias contas aborda todos esses desafios usando Contas da AWS compartimentalizadas para separar workloads e acesso.

Estrutura fundamental e responsabilidades de segurança para a transição para uma arquitetura de várias contas

As informações e as práticas recomendadas deste guia foram projetadas para complementar as recomendações da AWS existentes para infraestrutura e segurança. À medida que você faz a transição de uma única Conta da AWS para várias Contas da AWS, é importante garantir que sua nova arquitetura de várias contas seja consistente com os Princípios do AWS Well-Architected Framework e de base na nuvem. Isso ajuda a criar e operar um ambiente projetado para segurança, performance e resiliência ao mesmo tempo que cumpre os requisitos de governança e práticas recomendadas da AWS.

AWS Well-Architected Framework

O [AWS Well-Architected Framework](#) ajuda você a criar uma infraestrutura de alta performance que é segura, resiliente e eficiente para toda uma variedade de aplicações e workloads. Este guia se alinha aos pilares [Excelência operacional](#), [Segurança](#) e [Confiabilidade](#) dessa estrutura. 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.

Base na nuvem na AWS

O whitepaper da AWS [Estabelecer sua base na nuvem na AWS](#) fornece orientações para ajudar você a personalizar seu ambiente da AWS para atender às necessidades da sua empresa. Usando uma abordagem baseada em recursos, você pode criar um ambiente para implantar, operar e gerenciar suas workloads. Você também pode aprimorar os recursos para ampliar seu ambiente à medida que seus requisitos evoluem e você implanta workloads adicionais na nuvem. Para obter mais informações sobre os 30 recursos definidos pela AWS, consulte [Recursos](#). Este guia inclui práticas recomendadas para implementar os recursos iniciais na ordem pretendida.

Você pode adotar e implementar recursos de acordo com suas necessidades operacionais e de governança. À medida que seus requisitos de negócios amadurecem, a abordagem baseada em recursos pode ser usada como um mecanismo para verificar se seu ambiente de nuvem está pronto para suportar suas workloads e escalar conforme necessário. Essa abordagem permite a você estabelecer com confiança seu ambiente de nuvem para seus criadores e sua empresa.

Gerenciamento de identidade e controle de acesso para transição para uma arquitetura de várias contas

A primeira etapa ao fazer a transição para uma arquitetura de várias contas é configurar sua nova estrutura de contas dentro de uma organização. Em seguida, você poderá adicionar usuários e configurar o acesso às contas. Esta seção descreve abordagens para gerenciar o acesso humano em várias Contas da AWS.

Esta seção consiste nas seguintes tarefas:

- [Configurar uma organização](#)
- [Criar uma zona de pouso](#)
- [Adicionar unidades organizacionais](#)
- [Adicionar usuários iniciais](#)
- [Gerenciar contas-membro](#)

Configurar uma organização

Quando você tem várias Contas da AWS, é possível gerenciá-las logicamente por meio de uma organização no [AWS Organizations](#). Uma conta no AWS Organizations é uma Conta da AWS padrão que contém os seus recursos da AWS e as identidades que podem acessar esses recursos. Uma organização é uma entidade que consolida suas Contas da AWS para que você possa administrá-las como uma só unidade.

Quando você usa uma conta para criar uma organização, essa conta se torna a conta de gerenciamento (também conhecida como conta pagante ou conta raiz) para a organização. Uma organização só pode ter uma conta de gerenciamento. Quando você adiciona mais Contas da AWS à organização, elas se tornam contas-membro.

Note

Cada Conta da AWS também tem uma identidade única chamada usuário raiz. É possível fazer login como usuário raiz usando o endereço de e-mail e a senha usados para criar a conta. No entanto, recomendamos não usar o usuário raiz para suas tarefas diárias, nem

mesmo as administrativas. Para obter mais informações, consulte [usuário raiz da Conta da AWS](#).

Organize as contas em uma estrutura em forma de árvore hierárquica que consiste na raiz da organização, nas unidades organizacionais (OUs) e nas contas-membro. A raiz é o contêiner pai de todas as contas da sua organização. Uma unidade organizacional (OU) é um contêiner para [contas](#) dentro da [raiz](#). Uma OU pode conter outras OUs ou contas-membro. Uma OU pode ter apenas um pai, e cada conta pode ser um membro de apenas uma OU. Para obter mais informações, consulte [Terminologia e conceitos](#) (documentação do AWS Organizations).

Uma política de controle de serviços (SCP) especifica os serviços e ações que os usuários e perfis podem usar. As SCPs são semelhantes às políticas de permissão do AWS Identity and Access Management (IAM), exceto por não concederem permissões. Em vez disso, as SCPs definem as permissões máximas. Quando você anexa uma política a um dos nós na hierarquia, ela se aplica a todas as OUs e contas dentro desse nó. Por exemplo, se você aplicar uma política à raiz, ela se aplicará a todas as [OUs](#) e [contas](#) na organização, e se você aplicar uma política a uma OU, ela se aplicará somente às OUs e contas na OU de destino.

É possível usar o console do AWS Organizations para visualizar e gerenciar centralmente todas as suas contas dentro da organização. Um dos benefícios de usar uma organização é que você pode receber uma fatura consolidada que mostra todas as cobranças associadas às contas de gerenciamento e contas-membro. Para obter mais informações, consulte [Faturamento consolidado](#) na documentação do AWS Organizations.

Práticas recomendadas

- Não use uma Conta da AWS existente para criar uma organização. Comece com uma nova conta, a qual se tornará sua conta de gerenciamento para a organização. As operações privilegiadas podem ser executadas na conta de gerenciamento de uma organização, e os SCPs não se aplicam à conta de gerenciamento. É por isso que você deve limitar os recursos e dados da nuvem contidos na conta de gerenciamento somente àqueles que precisam ser gerenciados nessa conta.
- Limite o acesso à conta de gerenciamento somente às pessoas que precisam provisionar novas Contas da AWS e para administrar a organização.
- Use SCPs para definir as permissões máximas para a raiz, unidades organizacionais e contas-membro. As SCPs não podem ser aplicadas diretamente à conta de gerenciamento.
- Siga as [Práticas recomendadas do AWS Organizations](#) (documentação do AWS Organizations).

Criar uma zona de pouso

Uma zona de pouso é um ambiente da AWS com várias contas e bem arquitetado cujo objetivo é atuar como ponto de partida para a implantação de workloads e aplicações. Ele fornece uma linha de base para começar com arquitetura de várias contas, gerenciamento de identidade e acesso, governança, segurança de dados, design de rede e log. O [AWS Control Tower](#) é um serviço que simplifica a manutenção e a governança de um ambiente com várias contas por meio do fornecimento grades de proteção automatizadas. Normalmente, você provisiona uma única zona de pouso do AWS Control Tower que gerencia seu ambiente em todas as Regiões da AWS. O AWS Control Tower funciona orquestrando outros Serviços da AWS dentro da sua conta. Para obter mais informações, consulte [O que acontece quando você configura uma zona de pouso](#) (documentação do AWS Control Tower).

Ao configurar uma zona de pouso com o AWS Control Tower, você identifica três contas compartilhadas: a conta de gerenciamento, a conta de arquivamento de log e a conta de auditoria. Para obter mais informações, consulte [O que são contas compartilhadas](#) (documentação do AWS Control Tower). Para a conta de gerenciamento, você deve usar uma conta existente que não esteja hospedando nenhuma workload para configurar a zona de pouso. Para as contas de arquivamento de log e auditoria, é possível optar por reutilizar as Contas da AWS existentes, ou o AWS Control Tower pode criá-las para você.

Para obter instruções sobre como configurar sua zona de pouso do AWS Control Tower, consulte [Introdução](#) (documentação do AWS Control Tower).

Práticas recomendadas

- Siga as práticas recomendadas em [Princípios de design para sua estratégia de várias contas](#) (whitepaper da AWS).
- Siga as [Práticas recomendadas para administradores do AWS Control Tower](#) (documentação do AWS Control Tower).
- Crie sua zona de pouso na Região da AWS que hospeda a maioria das suas workloads.

Important

Se você decidir alterar a região depois de implantar sua zona de pouso, precisará da ajuda do AWS Support. Além disso, você também deverá descomissionar a zona de pouso. Esta prática não é recomendada.

- Ao determinar quais regiões o AWS Control Tower governará, selecione somente as regiões nas quais você espera implantar workloads imediatamente. É possível alterar essas regiões ou adicionar outras posteriormente. Se o AWS Control Tower governa uma região, ele implantará suas barreiras de proteção detectivas nessa região como [Regras do AWS Config](#).
- Depois de determinar quais regiões o AWS Control Tower governará, negue o acesso a todas as regiões não governadas. Isso ajuda a garantir que suas workloads e os desenvolvedores só possam usar as Regiões da AWS aprovadas. Isso é implementado como uma política de controle de serviços (SCP) na organização. Para obter mais informações, consulte [Configurar o controle de negação da Região da AWS](#) (documentação do AWS Control Tower).
- Ao configurar sua zona de pouso no AWS Control Tower, recomendamos renomear as seguintes OUs e contas:
 - Recomendamos renomear a OU Security para Security_Prod para significar que essa OU será usada para Contas da AWS relacionadas à segurança da produção.
 - Recomendamos permitir que o AWS Control Tower crie uma OU adicional e, em seguida, renomeá-la de Sandbox para Workloads. Na próxima seção, crie OUs adicionais na OU Workloads, a qual você usará para organizar suas Contas da AWS.
 - Recomendamos renomear o log centralizado Conta da AWS de Log Archive para log-archive-prod.
 - Recomendamos renomear a conta de auditoria de Audit para security-tooling-prod.
- Para ajudar a evitar fraudes, o AWS exige que as Contas da AWS tenham um histórico de uso antes que elas possam ser adicionadas a uma zona de pouso do AWS Control Tower. Se estiver usando uma nova Conta da AWS sem nenhum histórico de uso, você poderá iniciar na nova conta uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que não esteja no nível gratuito da AWS. Mantenha instância em execução por alguns minutos e, em seguida, encerre-a.

Adicionar unidades organizacionais

Estabelecer a estrutura organizacional adequada é fundamental para configurar um ambiente com várias contas. Como você usa políticas de controle de serviços (SCPs) para definir as permissões máximas para uma OU e as contas nela contidas, sua estrutura organizacional deve ser lógica do ponto de vista de gerenciamento, permissões e relatórios financeiros. Para obter mais informações sobre a estrutura de uma organização, incluindo unidades organizacionais (OUs), consulte [Terminologia e conceitos](#) (documentação do AWS Organizations).

Nesta seção, você personaliza a zona de pouso criando OUs aninhadas que ajudam a segmentar e estruturar seus ambientes, como produção e não produção. Essas práticas recomendadas foram desenvolvidas para segmentar sua zona de pouso a fim de separar recursos de produção e não produção e separar a infraestrutura das workloads.

Para obter mais informações sobre como criar OUs, consulte [Gerenciar unidades organizacionais](#) (documentação do AWS Organizations).

Práticas recomendadas

- Na OU Workloads que você criou em [Criar uma zona de pouso](#), crie as seguintes OUs aninhadas.
 - Prod: use essa OU para Contas da AWS que armazenam e acessam dados de produção, incluindo dados de clientes.
 - NonProd: use essa OU para Contas da AWS que armazenam dados de não produção, como ambientes de desenvolvimento, preparação ou teste

Na raiz da organização, crie uma OU Infrastructure_Prod. Use essa OU para hospedar uma conta de rede centralizada.

Adicionar usuários iniciais

Há duas maneiras de conceder às pessoas acesso a Contas da AWS:

- Identidades do IAM, como usuários, grupos e perfis
- Federação de identidades, por exemplo, usando o AWS IAM Identity Center

Em empresas menores e ambientes de conta única, é comum que os administradores criem um usuário do IAM quando uma nova pessoa entra na empresa. As credenciais da chave de acesso e da chave secreta associadas a um usuário do IAM são conhecidas como credenciais de longo prazo porque elas não expiram. No entanto, essa não é uma prática de segurança recomendada, pois se um invasor compromettesse essas credenciais, seria necessário gerar um novo conjunto de credenciais para o usuário. Outra abordagem para acessar Contas da AWS é por meio de [perfis do IAM](#). Também é possível usar o [AWS Security Token Service](#) (AWS STS) para solicitar temporariamente credenciais de curto prazo, as quais expiram após um período de tempo configurável.

É possível gerenciar o acesso de pessoas a suas Contas da AWS via [IAM Identity Center](#). Você pode criar contas de usuário individuais para cada um de seus funcionários ou contratados, eles podem gerenciar suas próprias senhas e soluções de autenticação multifator (MFA) e você pode agrupá-los para gerenciar o acesso. Ao configurar a MFA, é possível usar tokens de software, como aplicações autenticadoras, ou tokens de hardware, como dispositivos YubiKey.

O IAM Identity Center também oferece suporte à federação de provedores de identidade (IdPs) externos, como Okta, JumpCloud e Ping Identity. Para obter mais informações, consulte [Provedores de identidade compatíveis](#) (documentação do IAM Identity Center). Ao se federar com um IdP externo, você pode gerenciar a autenticação de usuários em todas as aplicações e, em seguida, usar o IAM Identity Center para autorizar o acesso a Contas da AWS específicas.

Práticas recomendadas

- Siga as [Práticas recomendadas de segurança](#) (documentação do IAM) para configurar o acesso de usuários.
- Gerencie o acesso à conta por meio de grupos em vez de usuários individuais. No IAM Identity Center, crie novos grupos para representar cada uma das suas funções comerciais. Por exemplo, é possível criar grupos para engenharia, finanças, vendas e gerenciamento de produtos.
- Muitas vezes, os grupos são definidos separando-se aqueles que precisam de acesso a todas as Contas da AWS (geralmente acesso somente leitura) e aqueles que precisam acessar uma única Conta da AWS. Recomendamos usar a convenção de nomenclatura a seguir para grupos a fim de facilitar a identificação da Conta da AWS e as permissões associadas ao grupo.

```
<prefix>-<account name>-<permission set>
```

- Por exemplo, para o grupo `AWS-A-dev-nonprod-DeveloperAccess`, `AWS-A` é um prefixo que indica acesso a uma única conta, `dev-nonprod` é o nome da conta e `DeveloperAccess` é o conjunto de permissões atribuído ao grupo. Para o grupo `AWS-0-BillingAccess`, o prefixo `AWS-0` indica acesso a toda a organização, enquanto `BillingAccess` indica o conjunto de permissões para o grupo. Neste exemplo, como o grupo tem acesso a toda a organização, o nome da conta não é representado no nome do grupo.
- Se você estiver usando o IAM Identity Center com um IdP externo baseado em SAML e quiser exigir MFA, poderá usar o controle de acesso por atributo (ABAC) para passar o método de autenticação do IdP para o IAM Identity Center. Os atributos são enviados por meio de declarações SAML. Para obter mais informações, consulte [Habilitar e configurar atributos para controle de acesso](#) (documentação do IAM Identity Center).

Muitos IdPs, como o Microsoft Azure Active Directory e o Okta, podem usar uma reivindicação do Authentication Method Reference (amr) dentro de uma declaração SAML para passar o status de MFA do usuário para o IAM Identity Center. A reivindicação usada para declarar o status de MFA e seu formato variam de acordo com o IdP. Para obter mais informações, consulte a documentação do seu IdP.

No IAM Identity Center, você pode então criar políticas de conjunto de permissões que determinam quem pode acessar seu recursos da AWS. Quando você habilita o ABAC e especifica atributos, o IAM Identity Center passa para o IAM o valor do atributo do usuário autenticado para uso na avaliação de políticas. Para obter mais informações, consulte [Criar políticas de permissão para o ABAC](#) (documentação do IAM Identity Center). Conforme mostrado no exemplo a seguir, é possível usar a chave de condição `aws:PrincipalTag` para criar uma regra de controle de acesso para MFA.

```
"Condition": {
  "StringLike": { "aws:PrincipalTag/amr": "mfa" }
}
```

Gerenciar contas-membro

Nesta seção, você convidará sua conta pré-existente para a organização e começará a criar novas contas dentro da organização. Uma parte importante desse processo é definir os critérios usados para determinar se é necessário provisionar uma nova conta.

Esta seção consiste nas seguintes tarefas:

- [Convidar sua conta pré-existente](#)
- [Personalizar as configurações da VPC no AWS Control Tower](#)
- [Definir os critérios de escopo](#)

Convidar sua conta pré-existente

No AWS Organizations, é possível convidar a conta pré-existente da sua empresa para sua nova organização. Somente a conta de gerenciamento da organização pode convidar outras contas para ingressar. Quando o administrador da conta convidada aceita o convite, a conta ingressa imediatamente na organização e a conta de gerenciamento da organização torna-se responsável

por todas as cobranças geradas pela nova conta-membro. Para obter mais informações, consulte [Convidar uma Conta da AWS para se juntar à sua organização](#) e [Aceitar ou recusar um convite de uma organização](#) (documentação do AWS Organizations).

Note

Você poderá convidar uma conta para ingressar em uma organização somente se essa conta não estiver em outra organização. Se a conta for membro de uma organização existente, será necessário removê-la da organização. Se a conta for a conta de gerenciamento de uma organização diferente que foi criada por engano, será necessário excluir a organização.

Important

Se precisar acessar qualquer informação histórica de custo ou uso da sua conta pré-existente, você poderá usar o AWS Cost and Usage Report para exportar essas informações para um bucket do Amazon Simple Storage Service (Amazon S3). Faça isso antes de aceitar o convite para ingressar na organização. Quando uma conta ingressa em uma organização, o acesso a esses dados históricos da conta é perdido. Para obter mais informações, consulte [Configurar um bucket do Amazon S3 para relatórios de custo e uso](#) (documentação do AWS Cost and Usage Report).

Práticas recomendadas

- Recomendamos adicionar sua conta preexistente, que provavelmente contém workloads de produção, à unidade organizacional Workloads > Prod criada em [Adicionar unidades organizacionais](#).
- Por padrão, a conta de gerenciamento da organização não tem acesso administrativo às contas-membro que são convidadas para a organização. Se desejar que a conta de gerenciamento tenha controle administrativo, será necessário criar o perfil do IAM OrganizationAccountAccessRole na conta-membro e conceder permissão à conta de gerenciamento para assumir o perfil. Para obter mais informações, consulte [Criar o perfil OrganizationAccountAccessRole em uma conta-membro convidada](#) (documentação do AWS Organizations).

- Para a conta pré-existente que você convidou para a organização, revise as [Práticas recomendadas para contas-membro](#) (documentação do AWS Organizations) e verifique se a conta segue essas recomendações.

Personalizar as configurações da VPC no AWS Control Tower

Recomendamos provisionar novas Contas da AWS via [Account Factory](#) no AWS Control Tower. Com o Account Factory, é possível usar a integração do AWS Control Tower com o Amazon EventBridge para provisionar recursos em novas Contas da AWS assim que a conta é criada.

Quando você configura uma nova Conta da AWS, uma [nuvem privada virtual \(VPC\) padrão](#) é provisionada automaticamente. No entanto, quando você configura uma nova conta via Account Factory, o AWS Control Tower provisiona automaticamente uma VPC adicional. Para obter mais informações, consulte [Visão geral do AWS Control Tower e VPCs](#) (documentação do AWS Control Tower). Isso significa que, por padrão, o AWS Control Tower provisiona duas VPCs padrão em cada nova conta.

É comum que as empresas queiram ter mais controle sobre as VPCs em suas contas. Muitas preferem usar outros serviços, como AWS CloudFormation, Hashicorp Terraform ou Pulumi, para configurar e gerenciar suas VPCs. Recomenda-se personalizar as configurações do Account Factory para evitar a criação da VPC adicional provisionada pelo AWS Control Tower. Para obter instruções, consulte [Configurar opções da Amazon VPC](#) (documentação do AWS Control Tower) e aplique as seguintes configurações:

1. Desabilite a opção Sub-rede acessível pela Internet.
2. Em Número de sub-redes privadas, escolha 0.
3. Em Regiões para criação de VPC, limpe todas as regiões.
4. Em Zonas de disponibilidade, escolha 3.

Práticas recomendadas

- Exclua a VPC padrão que é provisionada automaticamente em cada nova conta. Isso impede que os usuários iniciem instâncias públicas do EC2 na conta sem criar explicitamente uma VPC dedicada. Para obter mais informações, consulte [Excluir sub-redes e a VPC padrão](#) (documentação da Amazon Virtual Private Cloud). Você também pode configurar o [AWS Control Tower Account Factory para Terraform](#) (AFT) para excluir automaticamente a VPC padrão em contas recém-criadas.

- Provisione uma nova Conta da AWS chamada dev-nonprod na unidade organizacional Workloads > NonProd. Use essa conta para seu ambiente de desenvolvimento. Para obter instruções, consulte [Provisionar contas do Account Factory com o AWS Service Catalog](#) (documentação do AWS Control Tower).

Definir os critérios de escopo

É necessário selecionar os critérios que sua empresa usará ao decidir se deve provisionar uma nova Conta da AWS. Você pode decidir provisionar contas para cada unidade de negócios ou optar por provisionar contas com base no ambiente, como produção, teste ou controle de qualidade. Cada empresa tem seus próprios requisitos de quanto grandes ou pequenas suas Contas da AWS deveriam ser. Geralmente, você avalia os três fatores a seguir ao decidir como dimensionar suas contas:

- Equilíbrio das cotas de serviço: cotas de serviço são os valores máximos para o número de recursos, ações e itens para cada AWS service (Serviço da AWS) em uma Conta da AWS. Se várias workloads compartilharem a mesma conta e uma workload estiver consumindo a maior parte ou toda a cota de serviços, isso poderá afetar negativamente outra workload na mesma conta. Nesse caso, talvez seja necessário separar essas workloads em contas diferentes. Para obter mais informações, consulte [Cotas do AWS service \(Serviço da AWS\)](#) (Referência geral da AWS).
- Relatórios de custos: isolar workloads em contas separadas permite que você veja os custos em nível de conta nos relatórios de custo e uso. Ao usar a mesma conta para várias workloads, é possível utilizar tags para obter ajuda para gerenciar e identificar recursos. Para obter mais informações marcação com tags, consulte [Marcar recursos da AWS](#) (Referência geral da AWS).
- Controle de acesso: quando as workloads compartilham uma conta, é necessário considerar como as políticas do IAM serão configuradas para limitar o acesso aos recursos da conta de forma que os usuários não tenham acesso a workloads de que não precisam. Como alternativa, é possível usar várias contas e [conjuntos de permissões](#) no IAM Identity Center para gerenciar o acesso a contas individuais.

Práticas recomendadas

- Siga as práticas recomendadas em [Estratégia de várias contas da AWS para sua zona de pouso do AWS Control Tower](#) (documentação do AWS Control Tower).

- Estabeleça uma estratégia de marcação eficaz que ajude a identificar e gerenciar recursos da AWS. É possível usar tags para categorizar recursos por finalidade, unidade de negócios, ambiente ou outros critérios. Para obter mais informações, consulte [Práticas recomendadas para marcação com tags](#) (documentação do Referência geral da AWS).
- Não sobrecarregue uma conta com muitas workloads. Se a demanda da workload exceder uma cota de serviço, problemas de performance poderão ocorrer. É possível separar as workloads concorrentes em diferentes Contas da AWS ou solicitar um aumento da cota de serviço. Para obter mais informações, consulte [Solicitar um aumento de cota](#) (documentação do Service Quotas).

Gerenciar permissões e acesso para uma arquitetura de várias contas

Esta seção contém os seguintes tópicos:

- [Considerações culturais de engenharia](#)
- [Criar conjuntos de permissões](#)
- [Criar um limite de permissões](#)
- [Gerenciar permissões para indivíduos](#)

Considerações culturais de engenharia

Um dos pilares do AWS Well-Architected Framework é excelência operacional. As equipes devem entender o [modelo operacional](#) e seus papéis na obtenção de resultados de negócios. As equipes podem se concentrar em alcançar metas compartilhadas quando entendem suas responsabilidades, elas podem assumir a responsabilidade e saber como as decisões são tomadas.

Com empresas em estágio inicial que estão se desenvolvendo rapidamente, todos na equipe desempenham várias funções. Não é incomum que esses usuários tenham acesso altamente privilegiado a toda a Conta da AWS. À medida que as empresas crescem, elas geralmente querem seguir o princípio de privilégio mínimo e concedem somente as permissões necessárias para que o usuário faça seu trabalho. Para ajudar a limitar o escopo, é possível usar o [AWS Identity and Access Management Access Analyzer](#) para ver quais permissões um usuário ou um perfil do IAM está realmente usando. Isso possibilita remover qualquer excesso de permissões.

Talvez seja difícil decidir quem na sua empresa tem permissões para criar perfis do IAM. Isso geralmente é um vetor para escalar os privilégios. A escalada de privilégios ocorre quando um usuário pode expandir suas próprias permissões ou escopo de acesso. Por exemplo, se um usuário tem permissões limitadas, mas pode criar novos perfis do IAM, esse usuário pode escalar seus privilégios criando e assumindo um novo perfil do IAM que tenha a política gerenciada `AdministratorAccess` aplicada.

Algumas empresas limitam o provisionamento de perfis do IAM a uma equipe centralizada de pessoas confiáveis. A desvantagem dessa abordagem é que essa equipe pode rapidamente se tornar um gargalo, porque quase todos os Serviços da AWS exigem um perfil do IAM para operar. Como alternativa, você pode usar [limites de permissões](#) para delegar acesso ao IAM somente aos

usuários que estão desenvolvendo, testando, lançando e gerenciando sua infraestrutura de nuvem. Para obter exemplos de políticas, consulte [Exemplo de limites de permissão](#) (GitHub).

As equipes de operações de desenvolvimento (DevOps), também conhecidas como equipes de plataforma, muitas vezes precisam equilibrar os recursos de autoatendimento de várias equipes internas de desenvolvimento com a estabilidade operacional das aplicações. Promover uma cultura de engenharia que englobe autonomia, domínio e propósito no local de trabalho pode ajudar a motivar as equipes. Os engenheiros querem fazer seu trabalho de maneira autônoma, sem depender de outras pessoas para fazer as coisas por eles. Se as equipes de DevOps puderem implementar soluções de autoatendimento, isso também reduzirá a quantidade de tempo que outras pessoas dependem delas para fazer as coisas.

Criar conjuntos de permissões

É possível gerenciar o acesso à Conta da AWS por meio de [conjuntos de permissões](#) no AWS IAM Identity Center. Um conjunto de permissões é um modelo que ajuda a implantar uma ou mais políticas do IAM em várias Contas da AWS. Quando você atribui um conjunto de permissões a uma Conta da AWS, o IAM Identity Center cria um perfil do IAM e anexa suas políticas do IAM a esse perfil. Para obter mais informações, consulte [Criar e gerenciar conjuntos de permissão](#) (documentação do IAM Identity Center).

A AWS recomenda criar conjuntos de permissões que mapeiem as diferentes personas da sua empresa.

Por exemplo, você poderia criar os seguintes conjuntos de permissões:

- [Conjunto de permissões de faturamento](#)
- [Conjunto de permissões de desenvolvedor](#)
- [Conjunto de permissões de produção](#)

Os seguintes conjuntos de permissões são trechos de um modelo do AWS CloudFormation. Use esse código como ponto de partida e personalize-o para sua empresa. Para obter mais informações sobre modelos do CloudFormation, consulte [Saiba mais sobre noções básicas de modelos](#).

Conjunto de permissões de faturamento

A equipe financeira usa `BillingAccessPermissionSet` para visualizar o painel do console do AWS Billing e o AWS Cost Explorer em cada conta.

```

BillingAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to Billing and Cost Explorer
    InstanceArn: !Sub "arn:${AWS::Partition}:sso::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/Billing"
    Name: BillingAccess
    SessionDuration: PT8H
    RelayStateType: https://console.aws.amazon.com/billing/home

```

Conjunto de permissões de desenvolvedor

A equipe de engenharia usa DeveloperAccessPermissionSet para acessar contas de não produção.

```

DeveloperAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to provision resources through CloudFormation
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:ContinueUpdateRollback",
              "cloudformation:CreateChangeSet",
              "cloudformation:CreateStack",
              "cloudformation>DeleteStack",
              "cloudformation:RollbackStack",
              "cloudformation:UpdateStack"
            ]
          }
        ]
      }

```



```

    ],
    "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*",
    "Condition": {
      "ArnLike": {
        "cloudformation:RoleArn": "arn:${AWS::Partition}:iam:${!
aws:PrincipalAccount}:role/CloudFormationRole"
      },
      "Null": {
        "cloudformation:ImportResourceTypes": true
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "cloudformation:CancelUpdateStack",
      "cloudformation>DeleteChangeSet",
      "cloudformation:DetectStackDrift",
      "cloudformation:DetectStackResourceDrift",
      "cloudformation:ExecuteChangeSet",
      "cloudformation:TagResource",
      "cloudformation:UntagResource",
      "cloudformation:UpdateTerminationProtection"
    ],
    "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "cloudformation>CreateUploadBucket",
      "cloudformation:ValidateTemplate",
      "cloudformation:EstimateTemplateCost"
    ],
    "Resource": "*"
  }
]
}

```

InstanceArn: !Sub "arn:\${AWS::Partition}:sso::instance/ssoins-instanceId"

ManagedPolicies:

- !Sub "arn:\${AWS::Partition}:iam::aws:policy/AWSServiceCatalogEndUserFullAccess"
- !Sub "arn:\${AWS::Partition}:iam::aws:policy/AWSProtonDeveloperAccess"
- !Sub "arn:\${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
- !Sub "arn:\${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
- !Sub "arn:\${AWS::Partition}:iam::aws:policy/ReadOnlyAccess"

```
Name: DeveloperAccess
SessionDuration: PT8H
```

Conjunto de permissões de produção

A equipe de engenharia usa `ProductionPermissionSet` para acessar contas de produção. Esse conjunto de permissões tem acesso limitado, somente para visualização.

```
ProductionPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to production accounts
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:ContinueUpdateRollback",
            "Resource": "arn:${AWS::Partition}:cloudformation::*:stack/app/*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam:${!
aws:PrincipalAccount}:role/CloudFormationRole"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:CancelUpdateStack",
            "Resource": "arn:${AWS::Partition}:cloudformation::*:stack/app/*"
          }
        ]
      }
```

```

    ]
  }
  InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
  ManagedPolicies:
    - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
    - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
    - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/ViewOnlyAccess"
  Name: ProductionAccess
  SessionDuration: PT2H

```

Criar um limite de permissões

Após implantar os conjuntos de permissões, você estabelece um limite de permissões. O limite de permissões é um mecanismo para delegação de acesso ao IAM somente aos usuários que estão desenvolvendo, testando, lançando e gerenciando sua infraestrutura de nuvem. Esses usuários podem realizar somente as ações permitidas pela política e pelo limite de permissões.

Você pode definir o limite de permissões em um modelo do AWS CloudFormation e, em seguida, usar o CloudFormation StackSets para implantar o modelo em várias contas. Isso ajuda a estabelecer e manter políticas padronizadas em toda a organização com uma única operação. Para obter mais informações, consulte [Trabalhar com o AWS CloudFormation StackSets](#) (documentação do CloudFormation).

O modelo do CloudFormation a seguir provisiona um perfil do IAM e cria uma política do IAM que atua como um limite de permissões. Usando um conjunto de pilhas, é possível implantar esse modelo em todas as contas-membro da organização.

```

CloudFormationRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        Effect: Allow
        Principal:
          Service: !Sub "cloudformation.${AWS::URLSuffix}"
        Action: "sts:AssumeRole"
      Condition:
        StringEquals:
          "aws:SourceAccount": !Ref "AWS::AccountId"

```

```

Description: !Sub "DO NOT DELETE - Used by CloudFormation. Created by
CloudFormation ${AWS::StackId}"
ManagedPolicyArns:
  - !Sub "arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess"
PermissionsBoundary: !Ref DeveloperBoundary
RoleName: CloudFormationRole

DeveloperBoundary:
Type: "AWS::IAM::ManagedPolicy"
Properties:
Description: Permission boundary for developers
ManagedPolicyName: PermissionsBoundary
PolicyDocument:
Version: "2012-10-17"
Statement:
  - Sid: AllowModifyIamRolesWithBoundary
    Effect: Allow
    Action:
      - "iam:AttachRolePolicy"
      - "iam:CreateRole"
      - "iam>DeleteRolePolicy"
      - "iam:DetachRolePolicy"
      - "iam:PutRolePermissionsBoundary"
      - "iam:PutRolePolicy"
    Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
    Condition:
      ArnEquals:
        "iam:PermissionsBoundary": !Sub "arn:${AWS::Partition}:iam::
${AWS::AccountId}:policy/PermissionsBoundary"
  - Sid: AllowModifyIamRoles
    Effect: Allow
    Action:
      - "iam>DeleteRole"
      - "iam:TagRole"
      - "iam:UntagRole"
      - "iam:UpdateAssumeRolePolicy"
      - "iam:UpdateRole"
      - "iam:UpdateRoleDescription"
    Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
  - Sid: OverlyPermissiveAllowedServices
    Effect: Allow
    Action:
      - "lambda:*"
      - "apigateway:*"

```

```
- "events:*"  
- "s3:*"  
- "logs:*"  
Resource: "*"
```

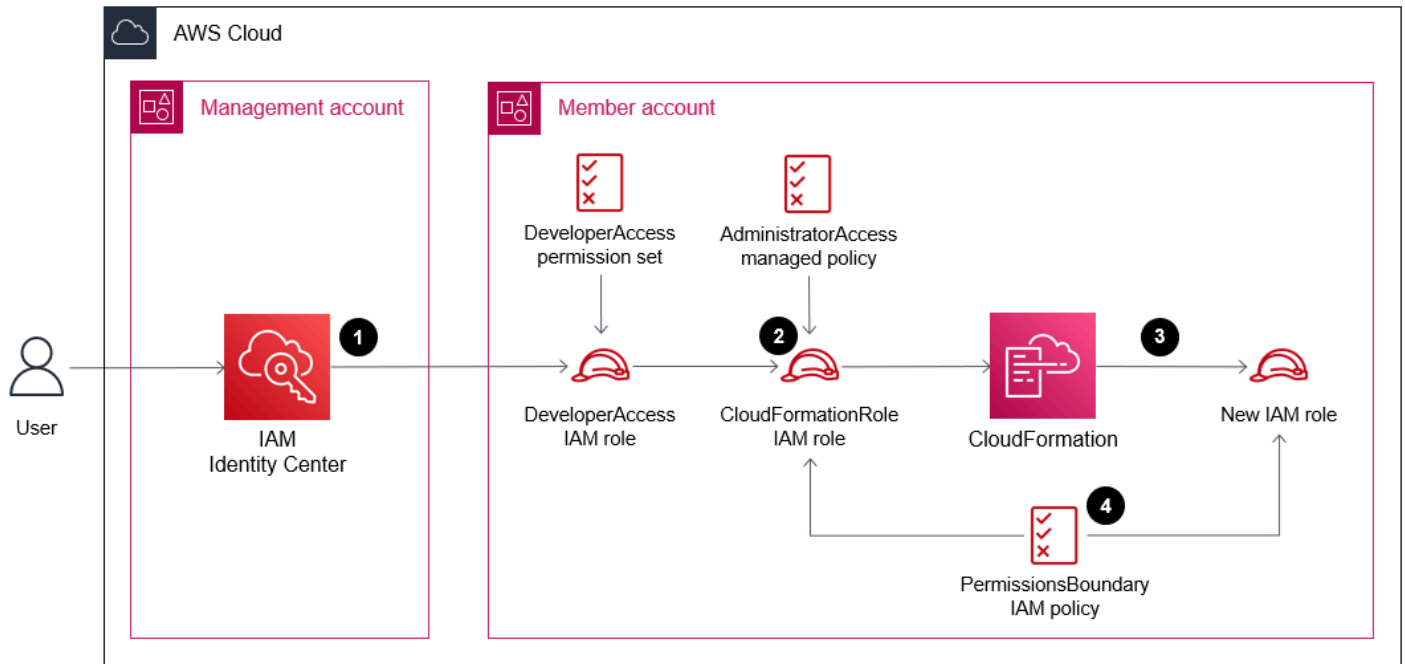
O perfil `CloudFormationRole`, a política `PermissionsBoundary` e o conjunto de permissões `DeveloperAccess` trabalham em conjunto para conceder as seguintes permissões:

- Usuários têm acesso somente de leitura à maioria dos Serviços da AWS por meio da política `ReadOnlyAccess` gerenciada pela AWS.
- Os usuários têm acesso a casos de suporte abertos por meio da política `AWSSupportAccess` gerenciada pela AWS.
- Usuários têm acesso somente leitura ao painel do console do AWS Billing por meio da política `AWSBillingReadOnlyAccess` gerenciada pela AWS.
- Os usuários podem provisionar novos ambientes via AWS Proton por meio da política `AWSProtonDeveloperAccess` gerenciada pela AWS.
- Os usuários podem provisionar produtos do Service Catalog por meio da política `AWSServiceCatalogEndUserFullAccess` gerenciada pela AWS.
- Os usuários podem validar e estimar o custo de qualquer modelo do CloudFormation por meio da política em linha.
- Ao usar o perfil do IAM `CloudFormationRole`, os usuários podem criar, atualizar ou excluir qualquer pilha do CloudFormation que comece com `app/`.
- Os usuários podem usar o CloudFormation para criar, atualizar ou excluir perfis do IAM que começam com `app/`. A política do IAM `PermissionsBoundary` impede que os usuários aumentem seus privilégios.
- Os usuários podem provisionar recursos do AWS Lambda, Amazon EventBridge, Amazon CloudWatch, Amazon Simple Storage Service (Amazon S3) e Amazon API Gateway somente com o CloudFormation.

A imagem a seguir mostra como um usuário autorizado, como um desenvolvedor, pode criar um novo perfil do IAM em uma conta-membro usando os conjuntos de permissões, perfis do IAM e limites de permissões descritos neste guia:

1. O usuário se autentica no IAM Identity Center e assume o perfil do IAM `DeveloperAccess`.
2. O usuário inicia a ação `cloudformation:CreateStack` e assume o perfil do IAM `CloudFormationRole`.

- O usuário inicia a ação `iam:CreateRole` e usa o CloudFormation para criar um novo perfil do IAM.
- A política do IAM `PermissionsBoundary` é aplicada ao novo perfil do IAM.



O perfil `CloudFormationRole` tem a política gerenciada [AdministratorAccess](#) anexada, mas devido à política do IAM `PermissionsBoundary`, as permissões efetivas do perfil `CloudFormationRole` tornam-se iguais à política `PermissionsBoundary`. A política `PermissionsBoundary` faz referência a si mesma ao permitir a ação `iam:CreateRole`, o que garante que os perfis possam ser criados somente se o limite de permissões for aplicado.

Gerenciar permissões para indivíduos

Usando conjuntos de permissões, o limite de permissões e o perfil do IAM `CloudFormationRole`, você pode limitar a quantidade de permissões que precisa atribuir diretamente a entidades principais individuais. Isso ajuda a gerenciar o acesso à medida que sua empresa cresce e a aplicar a prática recomendada de segurança de conceder privilégio mínimo.

Também é possível usar perfis vinculados ao serviço que concedem permissões a um serviço da AWS para provisionar recursos em seu nome. Em vez de conceder permissões à entidade principal do IAM (usuário, grupo de usuários ou perfil), é possível conceder as permissões ao serviço. Por exemplo, os perfis vinculados ao serviço para [AWS Proton](#) e [AWS Service Catalog](#) permitem que

você provisione seus próprios modelos, recursos e ambientes, sem atribuir permissões à entidade principal do IAM. Para obter mais informações, consulte [Serviços da AWS que funcionam com o IAM](#) e [Usar perfis vinculados ao serviço](#) (documentação do IAM).

Outra prática recomendada é limitar a quantidade de acesso que as pessoas têm ao AWS Management Console. Ao limitar o acesso ao console, é possível exigir que as pessoas provisionem recursos usando tecnologias de infraestrutura como código (IaC), como [AWS CloudFormation](#), [HashiCorp Terraform](#) ou [Pulumi](#). O gerenciamento da infraestrutura por meio de IaC permite rastrear alterações nos recursos ao longo do tempo e introduz mecanismos para aprovar mudanças, como as solicitações pull do GitHub.

Conectividade de rede para uma arquitetura de várias contas

Conectar VPCs

Muitas empresas usam o emparelhamento de VPC na Amazon Virtual Private Cloud (Amazon VPC) para conectar VPCs de desenvolvimento e produção. Usando uma conexão de emparelhamento de VPC, é possível rotear o tráfego entre duas VPCs usando endereçamento IP privado. As VPCs conectadas podem estar em diferentes Contas da AWS e diferentes Regiões da AWS. Para obter mais informações, consulte [O que é emparelhamento de VPC](#) (documentação da Amazon VPC). À medida que as empresas crescem e o número de VPCs aumenta, manter conexões emparelhadas entre todas as VPCs pode se tornar um desafio de manutenção. Você também pode ser limitado pelo número máximo de conexões de emparelhamento de VPC por VPC. Para obter mais informações, consulte [Cota de conexões de emparelhamento de VPC](#) (documentação da Amazon VPC).

Se você tiver vários ambientes de desenvolvimento, teste e preparação que hospedam dados que não sejam de produção em várias Contas da AWS, talvez você queira fornecer conectividade de rede entre todas essas VPCs, mas proibir qualquer acesso aos ambientes de produção. É possível usar o [AWS Transit Gateway](#) para conectar várias VPCs em várias contas. Você pode separar as tabelas de rotas para evitar que as VPCs de desenvolvimento se comuniquem com as VPCs de produção através do gateway de trânsito, o qual atua como um roteador centralizado. Para obter mais informações, consulte [Roteador centralizado](#) (documentação do Transit Gateway).

O Transit Gateway também oferece suporte ao emparelhamento com outros gateways de trânsito, incluindo aqueles em Contas da AWS ou Regiões da AWS diferentes. Como o Transit Gateway é um serviço totalmente gerenciado e altamente disponível, é necessário provisionar somente um gateway de trânsito para cada região.

Para obter mais informações e arquiteturas de rede detalhadas, consulte [Construindo uma infraestrutura de rede multi-VPC escalável e segura \(AWS Whitepaper\)](#).AWS

Conectar aplicações

Se precisar estabelecer comunicação entre aplicativos diferentes Contas da AWS no mesmo ambiente (como produção), você pode usar uma das seguintes opções:

- O [emparelhamento de VPC](#) ou o [AWS Transit Gateway](#) poderão fornecer conectividade em nível de rede se você desejar abrir um amplo acesso a vários endereços IP e portas.
- O [AWS PrivateLink](#) cria endpoints em uma sub-rede privada da VPC, e esses endpoints são registrados como entradas de DNS no [Amazon Route 53 Resolver](#). Ao usar o DNS, as aplicações podem resolver os endpoints e se conectar aos serviços registrados, sem exigir gateways NAT ou gateways da Internet na VPC.
- O [Amazon VPC Lattice](#) associa serviços, como aplicações em várias contas e VPCs e os reúne em uma rede de serviços. Os clientes em VPCs associadas à rede de serviços podem enviar solicitações para todos os outros serviços associados à rede de serviços, independentemente de estarem na mesma conta. O VPC Lattice se integra com AWS Resource Access Manager (AWS RAM) para que você possa compartilhar recursos com outras contas ou por meio de AWS Organizations. Uma VPC pode ser associada a apenas uma rede de serviços. Essa solução não requer o uso de emparelhamento de VPC ou AWS Transit Gateway para se comunicar entre contas.

Práticas recomendadas para conectividade de rede

- Crie um Conta da AWS que você use para a rede centralizada. Nomeie essa conta como network-prod e use-a para o AWS Transit Gateway Amazon [VPC IP](#) Address Manager (IPAM). Adicione esta conta à unidade organizacional Infrastructure_Prod.
- Use o [AWS Resource Access Manager](#) (AWS RAM) para compartilhar o gateway de trânsito, as redes de serviços VPC Lattice e os grupos do IPAM com o resto da organização. Isso permite que qualquer Conta da AWS pessoa da sua organização interaja com esses serviços.
- Ao usar grupos do IPAM para gerenciar centralmente as alocações de endereços IPv4 e IPv6, você pode permitir que seus usuários finais provisionem VPCs automaticamente usando [AWS Service Catalog](#). Isso ajuda a dimensionar adequadamente as VPCs e evitar a sobreposição de espaços de endereços IP.
- Use uma abordagem de saída centralizada para o tráfego vinculado à Internet e use uma abordagem de entrada descentralizada para o tráfego que entra em seu ambiente proveniente da Internet. Para obter mais informações, consulte [Saída centralizada](#) e [Entrada descentralizada](#).

Saída centralizada

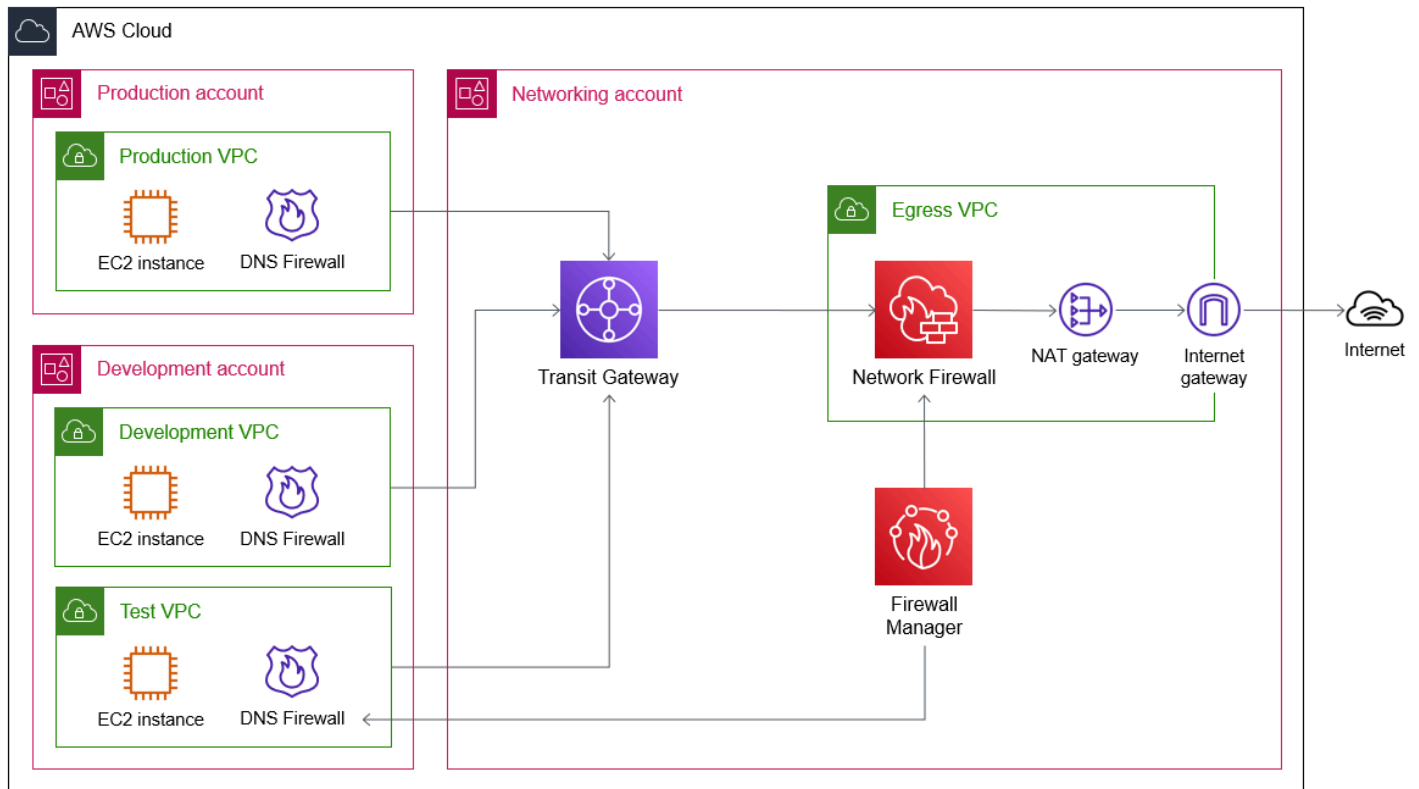
A saída centralizada é o princípio de usar um ponto de inspeção único e comum para todo o tráfego de rede destinado à Internet. Nesse ponto de inspeção, é possível permitir o tráfego somente para

domínios específicos ou somente por meio de portas ou protocolos especificados. A centralização da saída também pode ajudar a reduzir custos, eliminando a necessidade de implantar gateways NAT em cada uma de suas VPCs para acessar a Internet. Isso é benéfico do ponto de vista da segurança porque limita a exposição a recursos maliciosos acessíveis externamente, como a infraestrutura de comando e controle (C&C) de malware. Para obter mais informações e opções de arquitetura para saída centralizada, consulte Saída [centralizada para a Internet \(Whitepaper\)](#).AWS

Você pode usar o [AWS Network Firewall](#), que é um serviço stateful gerenciado de firewall de rede, detecção de invasões e prevenção, como um ponto de inspeção central para o tráfego de saída. Configure esse firewall em uma VPC dedicada para tráfego de saída. O Network Firewall oferece suporte a regras stateful que podem ser usadas para limitar o acesso à Internet a domínios específicos. Para obter mais informações, consulte [Lista de domínios](#) (documentação do Network Firewall).

Também é possível usar o [Amazon Route 53 Resolver DNS Firewall](#) para limitar o tráfego de saída a nomes de domínio específicos, principalmente para evitar a exfiltração não autorizada dos seus dados. Nas regras do DNS Firewall, é possível aplicar [listas de domínios](#) (documentação do Route 53) que permitem ou negam acesso a domínios especificados. Você pode usar listas de domínios AWS gerenciados, que contêm nomes de domínio associados a atividades maliciosas ou outras ameaças em potencial, ou você pode criar listas de domínios personalizadas. Crie grupos de regras do DNS Firewall e aplique-os às suas VPCs. As solicitações de DNS de saída são roteadas por meio de um resolvidor na VPC para resolução de nomes de domínio, e o DNS Firewall filtra as solicitações com base nos grupos de regras aplicados à VPC. As solicitações recursivas de DNS que vão para o resolvidor não fluem pelo gateway de trânsito e pelo caminho do Network Firewall. O Route 53 Resolver e o DNS Firewall devem ser considerados um caminho de saída separado para fora da VPC.

A imagem a seguir mostra um exemplo de arquitetura para saída centralizada. Antes do início da comunicação de rede, as solicitações de DNS são enviadas para o resolvidor do Route 53, onde o DNS Firewall permite ou nega a resolução do endereço IP usado para comunicação. O tráfego destinado à Internet é roteado para um gateway de trânsito em uma conta de rede centralizada. O gateway de trânsito encaminha o tráfego para o Network Firewall para inspeção. Se a política de firewall permitir o tráfego de saída, o tráfego será roteado por um gateway NAT, por um gateway da Internet e para a Internet. Você pode usar AWS Firewall Manager para gerenciar centralmente os grupos de regras do Firewall DNS e as políticas do Firewall de Rede em sua infraestrutura de várias contas.



Práticas recomendadas para proteger o tráfego de saída

- Comece no [modo somente de log](#) (documentação do Route 53). Mude para o modo de bloqueio depois de validar que o tráfego legítimo não é afetado.
- Bloqueie o tráfego de DNS que vai para a Internet usando [AWS Firewall Manager políticas para listas de controle de acesso à rede](#) ou usando AWS Network Firewall. Todas as consultas de DNS devem ser roteadas por meio de um Resolvedor do Route 53, onde você pode monitorá-las com a Amazon GuardDuty (se habilitado) e filtrá-las com o [Route 53 Resolver DNS Firewall](#) (se habilitado). Para obter mais informações, consulte [Resolver consultas ao DNS entre VPCs e sua rede](#) (documentação do Route 53).
- Use as [Listas de domínios gerenciadas pela AWS](#) (documentação do Route 53) no DNS Firewall e no Network Firewall.
- Considere bloquear domínios de alto nível não utilizados e de alto risco, como .info, .top, .xyz ou alguns domínios com código de país.
- Considere bloquear portas de alto risco não utilizadas, como as portas 1389, 4444, 3333, 445, 135, 139 ou 53.

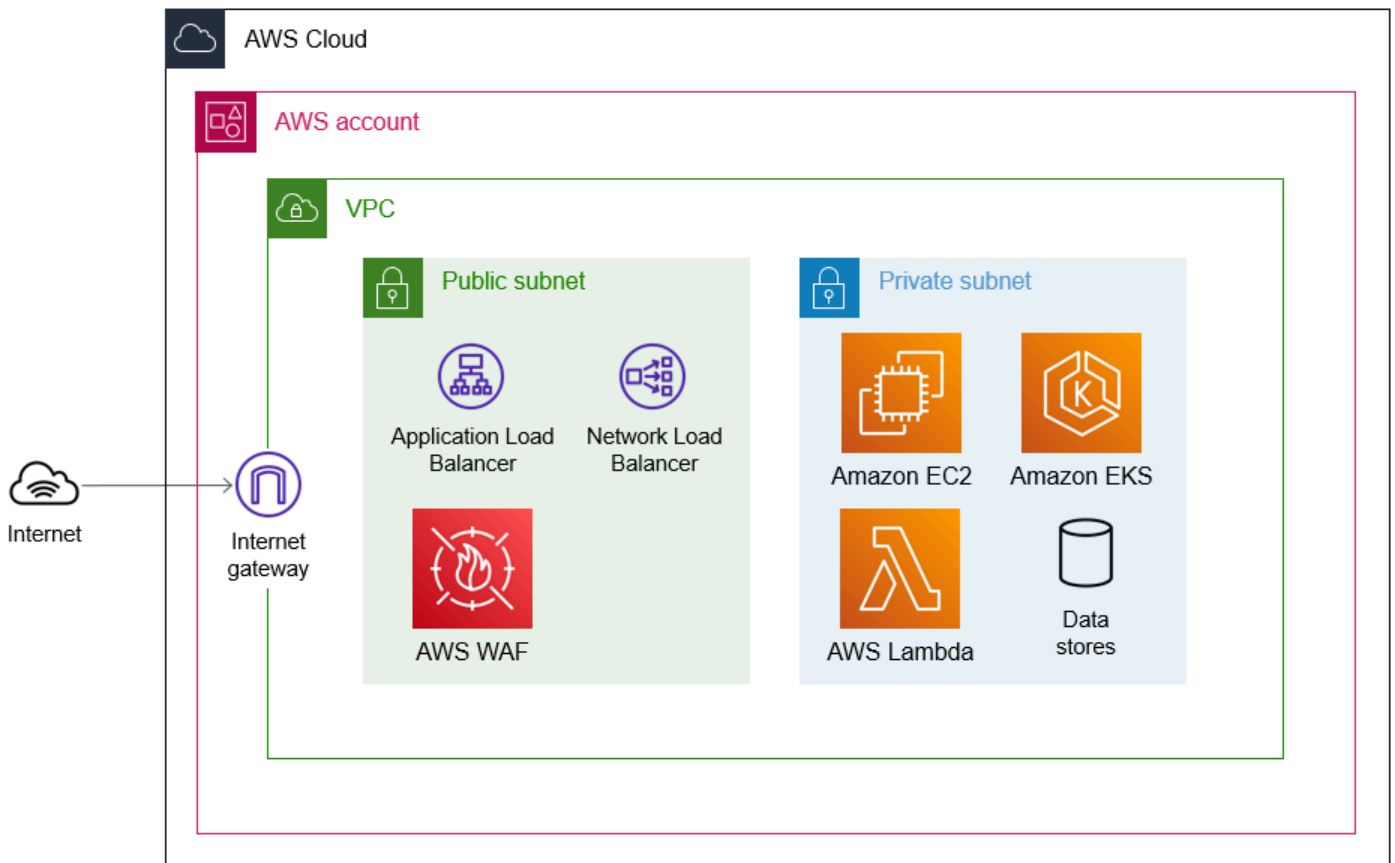
- Como ponto de partida, você pode usar uma lista de negação que inclui as regras AWS gerenciadas. Em seguida, você pode trabalhar ao longo do tempo para implementar um modelo de lista de permissões. Por exemplo, em vez de incluir somente uma lista restrita de nomes de domínio totalmente qualificados na lista de permissões, comece usando alguns curingas, como *.exemplo.com. Você pode até mesmo permitir apenas os domínios de nível superior que você espera e bloquear todos os outros. Então, com o tempo, reduza-os também.
- Use os [perfis do Route 53](#) (documentação do Route 53) para aplicar configurações do Route 53 relacionadas ao DNS em várias VPCs e em diferentes. Contas da AWS
- Defina um processo para lidar com exceções a essas melhores práticas.

Entrada descentralizada

Entrada descentralizada é o princípio de definir em nível de conta individual como o tráfego da Internet chega às workloads dessa conta. Em arquiteturas de várias contas, um dos benefícios da entrada descentralizada é que cada conta pode usar o serviço ou recurso de entrada mais adequado para suas workloads, como Application Load Balancer, Amazon API Gateway ou Network Load Balancer.

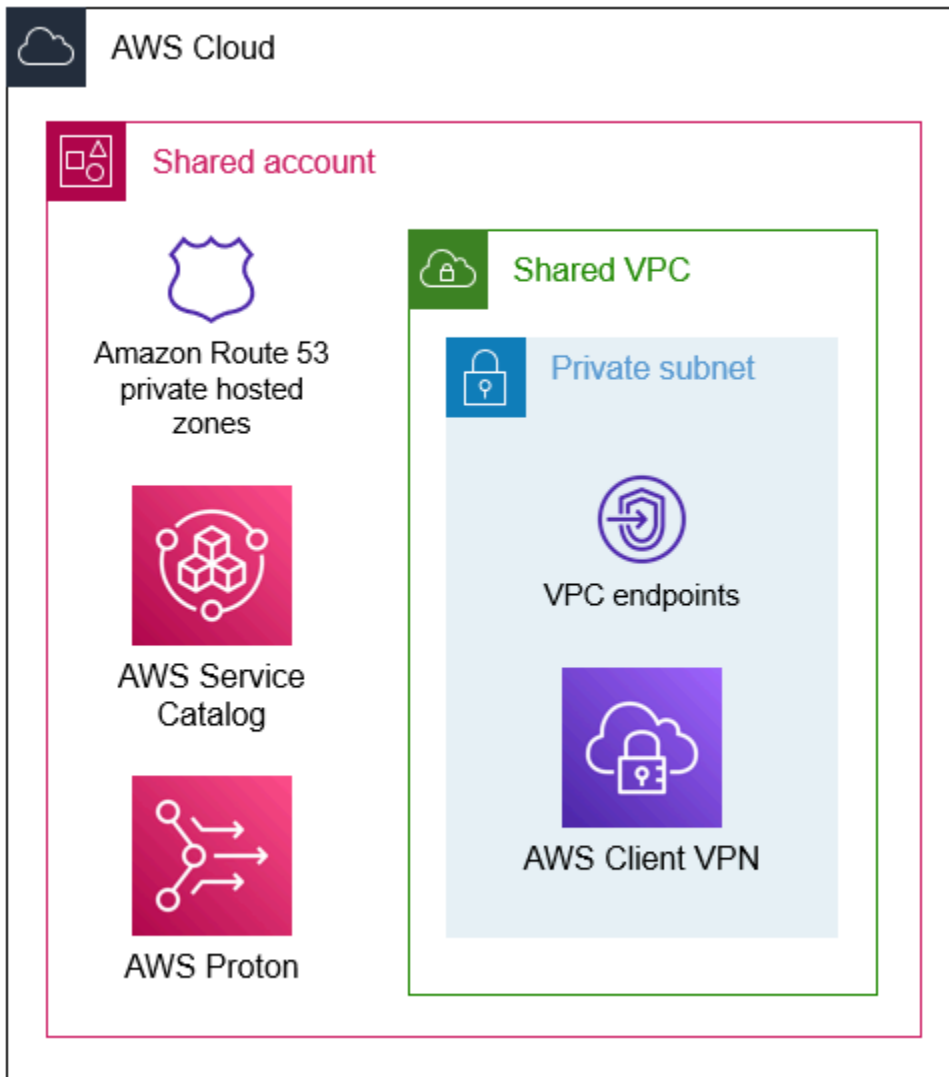
Embora a entrada descentralizada signifique que é necessário gerenciar cada conta individualmente, é possível administrar e manter centralmente suas configurações por meio do [AWS Firewall Manager](#). O Firewall Manager oferece suporte a proteções como o [AWS WAF](#) e [Grupos de segurança da Amazon VPC](#). Você pode se AWS WAF associar a um Application Load Balancer CloudFront, Amazon, API Gateway ou. AWS AppSync Se estiver usando uma VPC de saída e um gateway de trânsito, conforme descrito em [Saída centralizada](#), cada VPC spoke contém sub-redes públicas e privadas. No entanto, não há necessidade de implantar gateways NAT porque o tráfego passa pela VPC de saída na conta de rede.

A imagem a seguir mostra um exemplo de um indivíduo Conta da AWS que tem uma única VPC que contém uma carga de trabalho acessível pela Internet. O tráfego da Internet acessa a VPC por meio de um gateway da Internet e chega até os serviços de balanceamento de carga e segurança hospedados em uma sub-rede pública. (Uma sub-rede pública contém uma rota para um gateway da Internet.) Implante balanceadores de carga em sub-redes públicas e anexe listas de controle de AWS WAF acesso (ACLs) para ajudar na proteção contra tráfego malicioso, como scripts entre sites. Implante workloads que hospedam aplicações em sub-redes privadas sem acesso direto à Internet.



Se você tem muitas VPCs em sua organização, talvez queira compartilhar Serviços da AWS comuns criando endpoints da VPC de interface ou zonas hospedadas privadas em uma Conta da AWS dedicada e compartilhada. Para obter mais informações, consulte [Acessar e AWS service \(Serviço da AWS\) usar uma interface VPC endpoint](#) (AWS PrivateLink documentação) e [Trabalhar com zonas hospedadas privadas](#) (documentação do Route 53).

A imagem a seguir mostra um exemplo de uma Conta da AWS que hospeda recursos que podem ser compartilhados em toda a organização. Os endpoints da VPC podem ser compartilhados em várias contas quando são criados em uma VPC dedicada. Ao criar um endpoint da VPC, você pode opcionalmente fazer com que a AWS gerencie as entradas de DNS para o endpoint. Para compartilhar um endpoint, desmarque essa opção e crie as entradas de DNS em uma zona hospedada privada (PHZ) separada do Route 53. Em seguida, você pode associar o PHZ a todas as VPCs da sua organização para obter uma resolução centralizada de DNS dos endpoints da VPC. Também é necessário garantir que as tabelas de rotas do gateway de trânsito incluam rotas da VPC compartilhada para as outras VPCs. Para obter mais informações, consulte [Acesso centralizado aos endpoints AWS VPC da interface](#) (Whitepaper).



Um compartilhamento também Conta da AWS é um bom lugar para hospedar AWS Service Catalog portfólios. Um portfólio é uma coleção de serviços de TI que você deseja disponibilizar para implantação AWS, e o portfólio contém informações de configuração desses serviços. Você pode criar os portfólios na conta compartilhada, compartilhá-los com a organização e, em seguida, cada conta membro importa o portfólio para sua própria instância regional do Service Catalog. Para obter mais informações, consulte [Compartilhar com o AWS Organizations](#) (documentação do Service Catalog).

Da mesma forma, com AWS Proton, você pode usar a conta compartilhada para gerenciar centralmente seus modelos de ambiente e serviço e, em seguida, configurar conexões de conta com as contas dos membros da organização. Para obter mais informações, consulte [Conexões de conta de ambiente](#) (AWS Proton documentação).

Resposta a incidentes de segurança para uma arquitetura de várias contas

Ao fazer a transição para várias Contas da AWS, é importante manter a visibilidade dos eventos de segurança que podem ocorrer em sua organização. Em [Gerenciamento de identidade e controle de acesso](#), você usou o AWS Control Tower para configurar sua zona de pouso. Durante esse processo de configuração, AWS Control Tower designa uma Conta da AWS para segurança. Você deve delegar a administração dos serviços de segurança na security-tooling-prodconta e usar essa conta para gerenciar esses serviços de forma centralizada.

Este guia analisa o uso dos seguintes Serviços da AWS para ajudar a proteger suas Contas da AWS e sua organização:

- [Amazon GuardDuty](#)
- [Amazon Macie](#)
- [AWS Security Hub](#)

Amazon GuardDuty

O [Amazon GuardDuty](#) é um serviço contínuo de monitoramento de segurança que analisa fontes de dados, como registros de AWS CloudTrail eventos. Para obter uma lista completa das fontes de dados compatíveis, consulte [Como o Amazon GuardDuty usa suas fontes de dados](#) (GuardDuty documentação). Ele usa feeds de inteligência contra ameaças, como listas de endereços IP e domínios mal-intencionados, e machine learning para identificar atividades inesperadas, mal-intencionadas e possivelmente não autorizadas no seu ambiente da AWS .

Quando você usa GuardDuty com AWS Organizations, a conta de gerenciamento na organização pode designar qualquer conta na organização para ser o administrador GuardDuty delegado. O administrador delegado se torna a conta de GuardDuty administrador da Região. GuardDuty é habilitado automaticamente nessa Região da AWS, e a conta de administrador delegado tem permissões para habilitar e gerenciar GuardDuty todas as contas na organização dentro dessa região. Para obter mais informações, consulte [Gerenciamento de GuardDuty contas com AWS Organizations](#) (GuardDuty documentação).

GuardDuty é um serviço regional. Isso significa que você deve habilitar GuardDuty em cada região que deseja monitorar.

Práticas recomendadas

- Ativar GuardDuty em todos os compatíveis Regiões da AWS. GuardDuty pode gerar descobertas sobre atividades não autorizadas ou incomuns, mesmo em regiões que você não está usando ativamente. O preço do GuardDuty é baseado no número de eventos analisados. Mesmo em regiões onde você não está operando cargas de trabalho, a ativação GuardDuty é uma ferramenta de detecção eficaz e econômica para alertá-lo sobre atividades potencialmente maliciosas. Para obter mais informações sobre as regiões em que GuardDuty está disponível, consulte [Amazon GuardDuty Service Endpoints](#) (Referência geral da AWS).
- Em cada região, delegue a security-tooling-prodconta GuardDuty para administrar sua organização. Para obter mais informações, consulte [Designação de um administrador GuardDuty delegado](#) (GuardDuty documentação).
- Configure GuardDuty para inscrever automaticamente novas Contas da AWS à medida que forem adicionados à organização. Para obter mais informações, consulte Etapa 3 - automatizar a adição de novas contas da organização como membros em [Gerenciando contas com AWS Organizations](#) (GuardDuty documentação).

Amazon Macie

O [Amazon Macie](#) é um serviço de segurança e privacidade de dados totalmente gerenciado que usa machine learning e comparação de padrões para ajudar você a descobrir, monitorar e proteger dados confidenciais no Amazon Simple Storage Service (Amazon S3). Você pode exportar dados do Amazon Relational Database Service (Amazon RDS) e do Amazon DynamoDB para um bucket do S3 e depois usar o Macie para verificar os dados.

Quando você usa o Macie com AWS Organizations, a conta de gerenciamento na organização pode designar qualquer conta na organização como a conta de administrador do Macie. A conta do administrador pode habilitar e gerenciar o Macie para as contas-membros da organização, pode acessar dados de inventário do Amazon S3 e pode executar trabalhos confidenciais de descoberta de dados para as contas. Para obter mais informações, consulte [Gerenciar contas com o AWS Organizations](#) (documentação do Macie).

Macie é um serviço regional. Isso significa que você deve habilitar o Macie em cada região que deseja monitorar e que a conta de administrador do Macie só pode gerenciar contas-membros dentro da mesma região.

Práticas recomendadas

- Siga as [Considerações e recomendações para usar o Macie com o AWS Organizations](#) (documentação do Macie).
- Em cada região, delegue a security-tooling-prodconta para administrar o Macie para sua organização. Para gerenciar centralmente contas do Macie em várias Regiões da AWS, a conta de gerenciamento deve fazer login em cada região em que a organização atualmente usa ou usará o Macie e, em seguida, designar a conta de administrador do Macie em cada uma dessas regiões. A conta de administrador do Macie pode então configurar a organização em cada uma dessas regiões. Para obter mais informações, consulte [Integrar e configurar uma organização](#) (documentação do Macie).
- O Macie fornece um [nível gratuito mensal](#) para trabalhos de descoberta de dados confidenciais. Se você tiver dados confidenciais armazenados no Amazon S3, use o Macie para analisar seus buckets do S3 como parte do nível gratuito mensal. Se você exceder o nível gratuito, cobranças confidenciais de descoberta de dados começarão a ser acumuladas em sua conta.

AWS Security Hub

[AWS Security Hub](#) fornece uma visão abrangente do seu estado de segurança em AWS. Você pode usá-lo para verificar o ambiente segundo os padrões e as práticas recomendadas do setor de segurança. O Security Hub coleta dados de segurança de todos os seus Contas da AWS serviços (incluindo o GuardDuty Macie) e de produtos de parceiros terceirizados compatíveis. O Security Hub ajuda você a analisar tendências de segurança e identificar os problemas de segurança de prioridade mais alta. O Security Hub fornece vários padrões de segurança que você pode habilitar para realizar verificações de conformidade em cada Conta da AWS.

Quando você usa o Security Hub com AWS Organizations, a conta de gerenciamento na organização pode designar qualquer conta na organização como a conta de administrador do Security Hub. A conta de administrador do Security Hub pode então habilitar e gerenciar outras contas-membros na organização. Para obter mais informações, consulte [Usando AWS Organizations para gerenciar contas](#) (documentação do Security Hub).

O Security Hub é um serviço regional. Isso significa que você deve habilitar o Security Hub em cada região que deseja analisar e, em AWS Organizations, você deve definir o administrador delegado para cada região.

Práticas recomendadas

- Siga os [Pré-requisitos e recomendações](#) (documentação do Security Hub).
- Em cada região, delegue a security-tooling-prodconta para administrar o Security Hub da sua organização. Para obter mais informações, consulte [Designar uma conta de administrador do Security Hub](#) (documentação do Security Hub).
- Configure o Security Hub para inscrever automaticamente novos Contas da AWS quando eles forem adicionados à organização.
- Habilite o [AWS Foundational Security Best Practices standard](#)(documentação do Security Hub) para detectar quando os recursos se desviam das práticas recomendadas de segurança.
- Habilitar [Agregação entre regiões](#) (documentação do Security Hub) para que você possa visualizar e gerenciar todas as suas descobertas do Security Hub em uma única região.

Configurar backups para uma arquitetura de várias contas

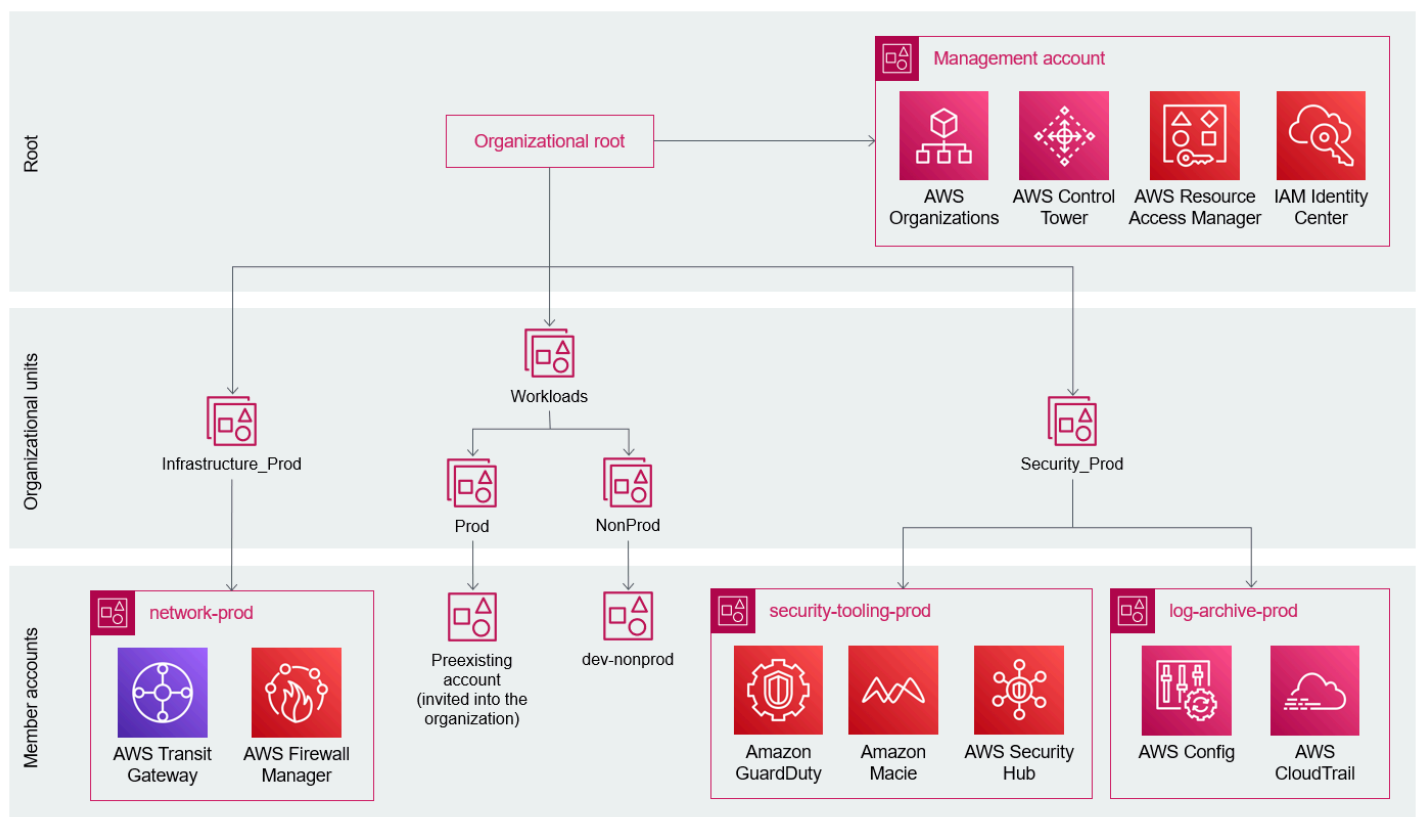
Uma estratégia abrangente de backup é uma parte essencial do plano de proteção de dados de uma empresa para resistir, se recuperar e reduzir qualquer impacto que possa ser causado por um evento de segurança. Uma política de backup ajuda a padronizar e implementar uma estratégia de backup para os recursos de todas as contas de sua organização. Em uma política de backup, você pode configurar e implantar planos de backup para seus recursos. Para obter mais informações, consulte [Políticas de backup](#) (documentação do AWS Organizations). Para obter mais informações, consulte [As 10 principais práticas recomendadas de segurança para proteger backups na AWS](#) (Recomendações da AWS).

Migração de contas ao fazer a transição para uma arquitetura de várias contas

Em [Convidar sua conta pré-existente](#), você convidou sua conta pré-existente para participar da unidade organizacional Workloads > Prod. Essa conta agora é gerenciada como parte da sua organização.

Você também provisionou uma nova conta dev-nonprod na unidade organizacional Workloads > NonProd. Os membros da equipe agora devem poder acessar as contas apropriadas via AWS IAM Identity Center. Remova todas as contas de usuário individuais no AWS Identity and Access Management(IAM).

Se você seguiu as recomendações deste guia, sua organização agora tem a estrutura a seguir.



Se houver workloads em execução na conta pré-existente, você agora deve migrar essas workloads para contas independentes de acordo com os critérios estabelecidos em [Definir os critérios de escopo](#). Migre qualquer workload de não produção para a nova unidade organizacional dev-nonprod

e migre as workloads de produção para a conta network-prod. Para obter mais informações sobre a migração de recursos da AWS comuns, consulte a seção a seguir deste guia, [Migração de recursos](#).

Replicação ou migração de recursos entre Contas da AWS

Depois de migrar de uma arquitetura de uma única conta Conta da AWS para várias contas, é comum ter cargas de trabalho de produção e não produção em execução na conta preexistente. A migração desses recursos para contas ou unidades organizacionais dedicadas de produção e não produção ajuda a gerenciar o acesso e a rede para essas workloads. Veja a seguir algumas opções para migrar AWS recursos comuns para outro Conta da AWS.

Esta seção tem como foco as estratégias para replicar dados entre Contas da AWS. Você deve se esforçar para que suas workloads sejam tão stateless quanto possível para evitar a necessidade de replicar recursos computacionais entre contas. Também é vantajoso gerenciar seus recursos por meio de infraestrutura como código (IaC) para que seja possível reprovisionar um ambiente em uma Conta da AWS separada.

Esta seção analisa as opções para migrar os seguintes recursos de dados:

- [AWS AppConfig configurações e ambientes](#)
- [AWS Certificate Manager certificados](#)
- [CloudFront Distribuições da Amazon](#)
- [AWS CodeArtifact domínios e repositórios](#)
- [Tabelas do Amazon DynamoDB](#)
- [EBSVolumes da Amazon](#)
- [EC2Instâncias da Amazon ou AMIs](#)
- [ECRRegistros da Amazon](#)
- [Sistemas de EFS arquivos da Amazon](#)
- [Clusters Amazon ElastiCache \(RedisOSS\)](#)
- [AWS Elastic Beanstalk ambientes](#)
- [Endereços IP elásticos](#)
- [AWS Lambda camadas](#)
- [Instâncias do Amazon Lightsail](#)
- [Clusters do Amazon Neptune](#)
- [OpenSearch Domínios do Amazon Service](#)
- [RDSInstantâneos da Amazon](#)
- [Clusters do Amazon Redshift](#)

- [Domínios e zonas hospedadas do Amazon Route 53](#)
- [Buckets do Amazon S3](#)
- [SageMaker Modelos da Amazon](#)
- [AWS WAF web ACLs](#)

AWS AppConfig configurações e ambientes

AWS AppConfig não suporta copiar diretamente sua configuração para outra Conta da AWS. No entanto, é uma prática recomendada gerenciar AWS AppConfig as configurações e os ambientes separadamente dos Contas da AWS que estão hospedando os ambientes. Para obter mais informações, consulte [Configuração entre contas com AWS AppConfig](#) (postagem AWS do blog).

AWS Certificate Manager certificados

Você não pode exportar diretamente um certificado AWS Certificate Manager (ACM) de uma conta para outra porque a chave AWS Key Management Service (AWS KMS) usada para criptografar a chave privada do certificado é exclusiva para cada Região da AWS conta. No entanto, é possível provisionar simultaneamente vários certificados com o mesmo nome de domínio em várias contas e regiões. ACM suporta a validação da propriedade do domínio usando DNS (recomendado) ou e-mail. Quando você usa a DNS validação e cria um novo certificado, ACM gera um CNAME registro exclusivo para cada domínio no certificado. O CNAME registro é exclusivo para cada conta e deve ser adicionado à zona hospedada ou ao DNS provedor do Amazon Route 53 em até 72 horas para que o certificado seja validado adequadamente.

CloudFront Distribuições da Amazon

A Amazon CloudFront não oferece suporte à migração de distribuições de uma Conta da AWS para outra Conta da AWS. No entanto, CloudFront suporta a migração de um nome de domínio alternativo, também conhecido como a CNAME, de uma distribuição para outra. Para obter mais informações, consulte [Como resolvo o CNAMEAlreadyExists erro ao configurar um CNAME alias para minha CloudFront distribuição](#) (Centro de AWS Conhecimento).

AWS CodeArtifact domínios e repositórios

Embora uma organização possa ter vários domínios, a recomendação é ter um único domínio de produção que contenha todos os artefatos publicados. Isso ajuda as equipes de desenvolvimento a

encontrar e compartilhar pacotes em toda a organização. O Conta da AWS proprietário do domínio pode ser diferente da conta que possui qualquer repositório associado ao domínio. É possível copiar pacotes entre repositórios, mas eles devem pertencer ao mesmo domínio. Para obter mais informações, consulte [Copiar pacotes entre repositórios](#) (CodeArtifact documentação).

Tabelas do Amazon DynamoDB

Você pode usar um dos seguintes serviços para migrar uma tabela do Amazon DynamoDB para uma Conta da AWS diferente:

- AWS Backup
- Importação e exportação do DynamoDB para o Amazon S3
- Amazon S3 e AWS Glue
- AWS Data Pipeline
- Amazon EMR

Para obter mais informações, consulte [Como posso migrar minhas tabelas do Amazon DynamoDB de uma para AWS outra \(Conta da AWS Centro de conhecimento\)](#).

EBSVolumes da Amazon

Você pode tirar um instantâneo de um volume existente do Amazon Elastic Block Store (AmazonEBS), compartilhar o instantâneo com a conta de destino e, em seguida, criar uma cópia do volume na conta de destino. Fazer isso migra efetivamente o volume de uma conta para outra. Para obter mais informações, consulte [Como posso compartilhar um EBS snapshot ou volume criptografado da Amazon com outro Conta da AWS](#) (Centro de AWS Conhecimento).

EC2Instâncias da Amazon ou AMIs

Não é possível transferir diretamente as instâncias existentes do Amazon Elastic Compute Cloud (AmazonEC2) ou Amazon Machine Images (AMIs) para outra Conta da AWS. Em vez disso, você pode criar uma personalização AMI na conta de origem, compartilhá-la AMI com a conta de destino, iniciar uma nova EC2 instância a partir da conta compartilhada AMI na conta de destino e cancelar o registro da compartilhada. AMI Para obter mais informações, consulte [Como faço para transferir uma EC2 instância da Amazon ou AMI para outra Conta da AWS](#) (Centro de AWS conhecimento).

ECR Registros da Amazon

O Amazon Elastic Container Registry (Amazon ECR) oferece suporte à replicação entre contas e entre regiões. Você configura a replicação no registro de origem e uma política de permissões do registro no registro de destino. Para obter mais informações, consulte [Configurar a replicação entre contas](#) (ECR documentação da Amazon) e [Permitir que o usuário raiz de uma conta de origem replique todos os repositórios](#) (documentação da Amazon). ECR

Sistemas de EFS arquivos da Amazon

Para o Amazon Elastic File System (Amazon EFS), você pode usar AWS DataSync para copiar dados de um sistema de arquivos de origem para um sistema de arquivos de destino em outra Conta da AWS. O DataSync agente deve ser criado no mesmo sistema de arquivos Região da AWS e Conta da AWS no sistema de arquivos de origem. Para obter mais informações, consulte [Transferência de dados de um sistema de arquivos na nuvem para outro sistema de arquivos na nuvem](#) (DataSync documentação). Ao copiar entre dois sistemas de EFS arquivos da Amazon em sistemas diferentes Contas da AWS, recomendamos que você use a transferência NFS (de origem) para EFS (de destino). Para obter mais informações e instruções, consulte [Criação de uma tarefa para transferir dados da Amazon EFS](#) (DataSync documentação).

Clusters Amazon ElastiCache (RedisOSS)

Você pode usar um backup de um cluster de banco de dados Amazon ElastiCache (RedisOSS) para migrá-lo para uma conta diferente. Para obter mais informações, consulte [Quais são as melhores práticas para migrar meu cluster ElastiCache \(RedisOSS\)](#) (Centro de AWS Conhecimento).

AWS Elastic Beanstalk ambientes

Para isso AWS Elastic Beanstalk, você pode usar [configurações salvas](#) (documentação do Elastic Beanstalk) para migrar um ambiente para outro. Conta da AWS Para obter mais informações, consulte [Como faço para migrar meu ambiente do Elastic Beanstalk de um Conta da AWS para outro \(Centro Conta da AWS de Conhecimento\)](#).AWS

Endereços IP elásticos

Você pode transferir endereços IP elásticos entre Contas da AWS e os mesmos Região da AWS. Para obter mais informações, consulte [Transferir endereços IP elásticos](#) (VPCdocumentação da Amazon).

AWS Lambda camadas

Por padrão, uma AWS Lambda camada que você cria é privada para você Conta da AWS. No entanto, você pode, opcionalmente, compartilhar a camada com outras pessoas Contas da AWS ou torná-la pública. Para copiar uma camada, você a reprovisiona em outra Conta da AWS. Para obter mais informações, consulte [Configurar permissões de camadas](#) (documentação do Lambda).

Instâncias do Amazon Lightsail

Você pode criar um snapshot de uma instância do Amazon Lightsail e exportá-lo para uma Amazon Machine Image (AMI) e um snapshot criptografado de um volume da Amazon. EBS Para obter mais informações, consulte [Exportação de snapshots do Amazon Lightsail para EC2 a Amazon \(documentação do Lightsail\)](#). Por padrão, o instantâneo é criptografado com uma chave AWS gerenciada criada em AWS Key Management Service (AWS KMS). No entanto, esse tipo de KMS chave não pode ser compartilhado entre eles Contas da AWS. Em vez disso, você criptografa manualmente uma cópia do AMI com uma chave gerenciada pelo cliente que pode ser usada na conta de destino. Para obter mais informações, consulte [Permitir que usuários de outras contas usem uma KMS chave](#) (AWS KMS documentação). Em seguida, você pode compartilhar o copiado AMI com o destino Conta da AWS e iniciar uma nova EC2 instância para o Lightsail a partir do copiado. AMI Para obter mais informações, consulte [Iniciar uma instância usando o novo assistente de inicialização de instância](#) (EC2documentação da Amazon).

Clusters do Amazon Neptune

Você pode copiar um snapshot automático do cluster de banco de dados Amazon Neptune para outra Conta da AWS. Para obter mais informações, consulte [Copiar um snapshot de cluster de banco de dados \(DB\)](#)(documentação do Neptune).

Você também pode compartilhar um snapshot manual com até 20 Contas da AWS , as quais podem restaurar um cluster de banco de dados desde o snapshot. Para obter mais informações, consulte [Compartilhar um snapshot de cluster de banco de dados](#)(documentação do Neptune).

OpenSearch Domínios do Amazon Service

Para copiar dados entre domínios do Amazon OpenSearch Service, você pode usar o Amazon S3 para criar um snapshot do domínio de origem e, em seguida, restaurar o snapshot em um domínio de destino em outro. Conta da AWS Para obter mais informações, consulte [Como faço para restaurar dados de um domínio do Amazon OpenSearch Service em outro Conta da AWS](#) (Centro de AWS Conhecimento).

Se você tiver conectividade de rede entre os Contas da AWS, também poderá usar o recurso de [replicação entre clusters](#) (documentação do OpenSearch serviço) no OpenSearch Serviço.

RDSInstantâneos da Amazon

Para o Amazon Relational Database Service (RDSAmazon), você pode compartilhar snapshots manuais de instâncias de banco de dados ou clusters com até 20.Contas da AWS Você poderá então restaurar a instância ou o cluster de banco de dados desde o snapshot compartilhado. Para obter mais informações, consulte [Como faço para compartilhar snapshots manuais de banco de RDS dados Amazon ou snapshots de cluster de banco de dados Aurora com Conta da AWS outra pessoa AWS \(Knowledge Center\)](#).

Você também pode usar AWS Database Migration Service (AWS DMS) para configurar a replicação contínua entre instâncias de banco de dados em contas diferentes. No entanto, isso requer conectividade de rede entre as contas, como VPC peering ou um gateway de trânsito.

Clusters do Amazon Redshift

Para migrar um cluster do Amazon Redshift para Conta da AWS outro, você cria um snapshot manual do cluster na conta de origem, compartilha o snapshot com o Conta da AWS destino e depois restaura o cluster a partir do snapshot. Para obter mais informações, consulte [Como faço para copiar um cluster provisionado do Amazon Redshift para outro Conta da AWS\(AWS Centro de conhecimento\)](#).

Domínios e zonas hospedadas do Amazon Route 53

É possível transferir domínios do Amazon Route 53 entre Contas da AWS. Para obter mais informações, consulte [Transferir um domínio para uma Conta da AWS diferente](#) (documentação do Route 53).

Você também pode migrar uma zona hospedada do Route 53 para outra Conta da AWS. Para obter mais informações sobre quando isso é recomendado ou exigido, consulte [Migrar uma zona hospedada para uma Conta da AWS diferente](#) (documentação do Route 53). Ao migrar uma zona hospedada, ela é recriada na Conta da AWS de destino. Para obter instruções, consulte [Migrar uma zona hospedada para uma Conta da AWS diferente](#) (documentação do Route 53).

Buckets do Amazon S3

Você pode usar a replicação na mesma região do Amazon Simple Storage Service (Amazon S3) para copiar objetos entre buckets do S3 na mesma região. Para obter mais informações, consulte [Replicar objetos](#) (documentação do Amazon S3). Observe o seguinte:

- Altere a propriedade da réplica para Conta da AWS a proprietária do bucket de destino. Para obter instruções, consulte [Alterar o proprietário da réplica](#) (documentação do Amazon S3).
- Atualize as condições do proprietário do bucket para refletir o Conta da AWS ID do bucket de destino. Para obter mais informações, consulte [Verificar a propriedade do bucket com a condição de proprietário do bucket](#) (documentação do Amazon S3).
- A partir de abril de 2023, a configuração imposta pelo proprietário do bucket está habilitada para buckets recém-criados, tornando ineficazes as listas de controle de acesso do bucket (ACLs) e o objeto ACLs. Para obter mais informações, consulte [As alterações de segurança do Amazon S3 estão chegando](#) (postagem AWS do blog).
- É possível usar a [Replicação em lote do S3](#) (documentação do Amazon S3) para replicar objetos que existiam antes da replicação ser configurada.

SageMaker Modelos da Amazon

SageMaker os modelos são armazenados em um bucket do Amazon S3 durante o treinamento. Ao conceder acesso ao bucket do S3 pela conta de destino, é possível implantar um modelo armazenado na conta de origem na conta de destino. Para obter mais informações, consulte [Como posso implantar um SageMaker modelo da Amazon em outro Conta da AWS](#) (Centro de AWS conhecimento).

AWS WAF web ACLs

AWS WAF as listas de controle de acesso à web (webACLs) devem residir na mesma conta dos recursos aos quais estão associadas, como CloudFront distribuições da Amazon, Application Load

Balancers, Amazon API Gateway e REST APIs AWS AppSync GraphQL. APIs Você pode usar AWS Firewall Manager para gerenciar centralmente a AWS WAF web ACLs em toda a sua organização dentro AWS Organizations e entre regiões. Para obter mais informações, consulte [Conceitos básicos de políticas do AWS Firewall Manager do AWS WAF](#) (documentação do Firewall Manager).

Considerações de cobrança ao fazer a transição para uma arquitetura de várias contas

Se você usar AWS Organizations para fazer a transição para várias Contas da AWS, poderá usar o [recurso de faturamento consolidado](#) (AWS Organizations documentação). Esse recurso fornece uma fatura única e combinada que mostra as cobranças em várias contas.

A seguir estão as melhores práticas de cobrança e recomendações para a transição para várias contas:

- Se você precisar acessar seus dados históricos de faturamento, antes de aceitar o convite para se juntar a uma organização, crie um [relatório de custos e uso](#) (AWS Cost and Usage Report documentação) para exportar os dados históricos de faturamento da conta para um bucket do Amazon Simple Storage Service (Amazon S3). Depois de aceitar o convite para participar da organização, os dados históricos de faturamento da conta não estarão mais acessíveis.
- Se precisar combinar duas organizações, como para uma fusão ou aquisição, você pode usar a [Avaliação de Conta para AWS Organizations \(Biblioteca de AWS Soluções\) para](#) avaliar as políticas baseadas em recursos em cada organização e identificar possíveis problemas antes de combiná-las.

Conclusão

A transição de uma única Conta da AWS para várias contas pode parecer difícil no início sem uma estratégia de adoção. Ao implementar uma estratégia de várias contas, é possível abordar muitos dos desafios enfrentados pelas empresas ao usar uma única Conta da AWS:

- **Confundir dados de produção com dados de desenvolvimento:** é possível conceder permissões e acessos diferentes usando o AWS IAM Identity Center com conjuntos de permissões separados e unidades organizacionais de produção e não produção. Somente usuários altamente privilegiados devem ter acesso ao banco de dados de produção, e esse acesso deve ser por períodos limitados e auditado.
- **Implantação de produção afetando outras operações comerciais:** é possível separar as partes interessadas usando várias contas e vários ambientes. Por exemplo, você pode criar um ambiente de demonstração de vendas dedicado, dentro de uma conta de não produção, para poder planejar implantações e lançamentos quando demonstrações não estiverem ocorrendo.
- **Performance insatisfatória da workload de produção ao testar workloads de desenvolvimento:** cada Conta da AWS tem cotas de serviço independentes que regem cada serviço. Ao usar várias contas, é possível limitar o escopo de um ambiente que afeta outro ambiente.
- **Distinguir os custos de produção dos custos de desenvolvimento:** o faturamento consolidado da organização acumula todos os custos no nível da Conta da AWS para que a equipe financeira possa ver quanto custa a produção em comparação com ambientes de não produção, como ambientes de desenvolvimento, teste e demonstração. Também é possível usar tags e políticas de marcação para separar os custos em uma conta.
- **Limitar o acesso a dados confidenciais:** o IAM Identity Center permite a utilização de políticas de acesso separadas para um grupo de pessoas associadas a uma conta específica.
- **Controle de custos:** ao usar políticas de controle de serviços (SCPs) em uma arquitetura de várias contas, você pode proibir o acesso a determinados Serviços da AWS que poderiam gerar custos elevados para sua organização. Os SCPs podem negar todo o acesso a serviços específicos ou limitar o uso de um serviço a um tipo específico, como restringir os tipos de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que podem ser criadas.

Colaboradores

Os colaboradores deste documento incluem:

- Justin Plock, arquiteto de soluções principal, AWS (autor principal)
- Emily Arnautovic, arquiteta principal, AWS
- Jason DiDomenico, arquiteto sênior de soluções, AWS
- Michael Leighty, arquiteto sênior de soluções especialista em segurança, AWS
- Jesse Lepich, arquiteto sênior de soluções especializado em segurança, AWS
- Rodney Lester, arquiteto principal de soluções, AWS
- Israel Lopez Moriano, arquiteto de soluções, AWS
- George Rolston, arquiteto sênior de soluções, AWS
- Alex Torres, arquiteto sênior de soluções, AWS
- Dave Walker, arquiteto principal de soluções, AWS

Recursos

Recomendações da AWS

- [AWS Startup Security Baseline \(AWS SSB\)](#)
- [AWS Security Reference Architecture \(AWS SRA\)](#)
- [As 10 principais práticas recomendadas de segurança para proteger backups na AWS](#)

Publicações no blog da AWS

- [Como a configuração de usuários e funções do IAM pode ajudar a manter sua startup segura](#)
- [Como permitir que os criadores desenvolvam recursos de IAM e, ao mesmo tempo, melhorem a segurança e a agilidade de sua organização](#)

Whitepapers da AWS

- [Organizar seu ambiente da AWS usando várias contas](#)
- [Estabelecer sua base de nuvem na AWS](#)
- [Construção de uma infraestrutura de rede da AWS Multi-VPC escalável e segura](#)

Exemplos de código da AWS

- [Automatize a configuração de serviços de segurança com o AWS Control Tower \(GitHub\)](#)

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
Melhores práticas de saída centralizada	Atualizamos as melhores práticas para proteger o tráfego de saída.	6 de maio de 2024
Práticas recomendadas para organizações	Atualizamos as práticas recomendadas para criar uma organização no AWS Organizations.	4 de dezembro de 2023
Considerações sobre cobrança	Adicionamos a seção Considerações sobre cobrança .	20 de setembro de 2023
Migração de recursos, conectividade de aplicações e Amazon VPC Lattice	Adicionamos a seções Migração de recursos e Conexão de aplicação s . Também adicionamos informações sobre um novo AWS service (Serviço da AWS), o Amazon Virtual Private Cloud (Amazon VPC) Lattice.	27 de abril de 2023
Histórico da conta e ABAC	Revisamos a seção Criar uma zona de pouso para adicionar informações sobre como garantir que sua nova Contas da AWS tenha histórico de uso para que você possa adicioná-la à sua zona de AWS Control	6 de janeiro de 2023

Tower pouso. Também revisamos a seção [Adicionar usuários iniciais](#) para adicionar informações sobre como usar o controle de acesso por atributo (ABAC) para passar o método de autenticação de um IdP baseado em SAML externo para o AWS IAM Identity Center.

[Rede de tráfego de saída](#)

Revisamos a seção de [saída centralizada](#) para adicionar informações sobre o uso do Firewall Amazon Route 53 Resolver DNS para limitar o tráfego de saída a nomes de domínio específicos.

13 de outubro de 2022

[Segurança do tráfego de saída](#)

Adicionamos [Práticas recomendadas para proteger o tráfego de saída](#).

6 de outubro de 2022

[Limites de permissões](#)

Melhoramos a definição de [limite de permissões](#) e, na seção Recursos, adicionamos um novo link para mais informações sobre esse tópico.

22 de setembro de 2022

[Publicação inicial](#)

—

6 de setembro 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: migre seu banco de dados Oracle local para a edição compatível com Amazon Aurora PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape)]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Amazon Relational Database Service (AmazonRDS) for Oracle no. Nuvem AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migre seu sistema de gerenciamento de relacionamento com o cliente (CRM) para a Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift]) mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Oracle em uma EC2 instância no. Nuvem AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma local para um serviço em nuvem para a mesma plataforma. Exemplo: migrar um Microsoft Hyper-V aplicativo para o. AWS
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um

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

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

A

ABAC

Consulte controle de [acesso baseado em atributos](#).

serviços abstratos

Veja os [serviços gerenciados](#).

ACID

Veja [atomicidade, consistência, isolamento, durabilidade](#).

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja a [inteligência artificial](#).

AIOps

Veja as [operações de inteligência artificial](#).

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade () ACID

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

controle de acesso baseado em atributos () ABAC

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

fonte de dados autorizada

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

Availability Zone (zona de disponibilidade)

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

AWS Estrutura de adoção da nuvem (AWS CAF)

Uma estrutura de diretrizes e melhores práticas AWS para ajudar as organizações a desenvolver um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS 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, AWS CAF fornece orientação para desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o [AWS CAFsite](#) e o [AWS CAFwhitepaper](#).

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

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS 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. Você pode usar um gráfico de comportamento com o Amazon Detective para examinar tentativas de login malsucedidas, API chamadas suspeitas e ações semelhantes. Para obter mais informações, consulte [Dados em um gráfico de comportamento](#) na documentação do Detective.

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também [endianness](#).

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

acesso em vidro quebrado

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção [Organizados de acordo com as capacidades de negócios](#) do whitepaper [Executar microsserviços containerizados na AWS](#).

planejamento de continuidade de negócios () BCP

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

C

CAF

Consulte [Estrutura de adoção da AWS nuvem](#).

implantação canária

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

CCoE

Veja o [Centro de Excelência em Nuvem](#).

CDC

Veja [a captura de dados de alterações](#).

alterar captura de dados (CDC)

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

engenharia do caos

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

CI/CD

Veja a [integração e a entrega contínuas](#).

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendadas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as [CCoEpostagens](#) no blog de estratégia Nuvem AWS corporativa.

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

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

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação — Fazer investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma landing zone, definir uma 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 de estratégia Nuvem AWS empresarial. Para obter

informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o [guia de preparação para migração](#).

CMDB

Consulte o [banco de dados de gerenciamento de configuração](#).

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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 YAML modelo. Para obter mais informações, consulte [Pacotes de conformidade na documentação](#). AWS Config

integração contínua e entrega contínua (CI/CD)

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

CV

Veja [visão computacional](#).

D

dados em repouso

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

classificação de dados

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

desvio de dados

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

dados em trânsito

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

malha de dados

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de banco de dados (DDL)

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

linguagem de manipulação de banco de dados () DML

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

DDL

Consulte a [linguagem de definição de banco](#) de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

implantação

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

ambiente de desenvolvimento

Veja o [ambiente](#).

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

Um processo usado para identificar e priorizar restrições que afetam negativamente a velocidade e a qualidade em um ciclo de vida de desenvolvimento de software. 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 (RD)

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

DML

Veja a [linguagem de manipulação de banco](#) de dados.

design orientado por domínio

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

DR

Veja a [recuperação de desastres](#).

detecção de deriva

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

DVSM

Veja o [mapeamento do fluxo de valor do desenvolvimento](#).

E

EDA

Veja a [análise exploratória de dados](#).

computação de borda

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

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o [endpoint do serviço](#).

serviço de endpoint

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

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

environment (ambiente)

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

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

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

epic

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

ERP

Veja o [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. EDA é realizado calculando estatísticas resumidas e criando visualizações de dados.

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a [filial](#).

recursos

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

importância do recurso

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

transformação de recursos

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

FGAC

Veja o [controle de acesso refinado](#).

controle de acesso refinado () FGAC

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

migração flash-cut

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

G

bloqueio geográfico

Veja as [restrições geográficas](#).

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

estratégia greenfield

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

barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais (OUs). Barreiras de proteção preventivas impõem políticas para garantir o alinhamento a padrões de conformidade. Eles são implementados usando políticas de controle de serviços e limites de IAM permissões. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a [alta disponibilidade](#).

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

Imediatamente após a substituição, o período em que uma equipe de migração gerencia e monitora as aplicações migradas na nuvem para resolver quaisquer problemas. Normalmente,

a duração desse período é de 1 a 4 dias. No final do período de hipercuidados, a equipe de migração normalmente transfere a responsabilidade pelas aplicações para a equipe de operações de nuvem.

I

IaC

Veja a [infraestrutura como código](#).

Política baseada em identidade

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

aplicação ociosa

Um aplicativo que tem uma média CPU de uso de memória entre 5 e 20 por cento em um período de 90 dias. Em um projeto de migração, é comum retirar essas aplicações ou retê-las on-premises.

IIoT

Veja a [Internet das Coisas industrial](#).

infraestrutura imutável

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

entrada (entrada) VPC

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

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente

I

apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

inspeção VPC

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

Internet das Coisas (IoT)

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

interpretabilidade

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

IoT

Consulte [Internet das Coisas](#).

Biblioteca de informações de TI (ITIL)

Um conjunto de práticas recomendadas para fornecer serviços de TI e alinhar esses serviços a requisitos de negócios. ITIL fornece a base para 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 ITSM ferramentas, consulte o [guia de integração de operações](#).

ITIL

Consulte [a biblioteca de informações](#) de TI.

ITSM

Veja o [gerenciamento de serviços de TI](#).

L

controle de acesso baseado em etiquetas () LBAC

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

zona de pouso

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

informações sobre zonas de pouso, consulte [Configurar um ambiente da AWS com várias contas seguro e escalável](#).

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de [acesso baseado em rótulos](#).

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja [7 Rs](#).

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também [endianness](#).

ambientes inferiores

Veja o [ambiente](#).

M

machine learning (ML)

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

ramificação principal

Veja a [filial](#).

malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vazar informações confidenciais ou obter acesso

não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Tróia, spyware e keyloggers.

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte [Migration Acceleration Program](#).

mecanismo

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

conta-membro

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

MES

Veja o [sistema de execução de manufatura](#).

Transporte de telemetria de enfileiramento de mensagens () MQTT

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

microsserviço

Um serviço pequeno e independente que se comunica de forma bem definida APIs e normalmente é de propriedade de equipes pequenas e independentes. Por exemplo, um sistema de seguradora pode incluir microsserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios

dos microsserviços incluem agilidade, escalabilidade flexível, fácil implantação, código reutilizável e resiliência. Para obter mais informações, consulte [Integração de microsserviços usando serviços sem AWS servidor](#).

arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio de uma interface bem definida usando leveza. APIs Cada microsserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte [Implementação de microsserviços em. AWS](#)

Programa de Aceleração de Migração (MAP)

Um AWS programa que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a compensar o custo inicial das migrações. 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: rehoste a migração para a Amazon EC2 com o AWS Application Migration Service.

Avaliação do portfólio de migração (MPA)

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

Avaliação da prontidão para migração () MRA

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

estratégia de migração

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

ML

Veja o [aprendizado de máquina](#).

modernização

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

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um

esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte [Avaliação da prontidão para modernização de aplicativos](#) no. Nuvem AWS

aplicações monolíticas (monólitos)

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

MPA

Consulte [Avaliação do portfólio de migração](#).

MQTT

Consulte Transporte de [telemetria de enfileiramento de](#) mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja o [controle de acesso de origem](#).

OAI

Veja a [identidade de acesso de origem](#).

OCM

Veja o [gerenciamento de mudanças organizacionais](#).

migração offline

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

OI

Veja a [integração de operações](#).

OLA

Veja o [contrato em nível operacional](#).

migração online

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

OPC-EUA

Consulte [Comunicação de processo aberto — Arquitetura unificada](#).

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

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

acordo de nível operacional () OLA

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

análise de prontidão operacional () ORR

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

tecnologia operacional (OT)

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

integração de operações (OI)

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

trilha organizacional

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

gestão de mudanças organizacionais (OCM)

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

controle de acesso de origem (OAC)

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

identidade de acesso de origem (OAI)

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

ORR

Veja a [análise de prontidão operacional](#).

NÃO

Veja a [tecnologia operacional](#).

saída (saída) VPC

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

P

limite de permissões

Uma política IAM de gerenciamento anexada aos IAM diretores para definir as permissões máximas que o usuário ou a função podem ter. Para obter mais informações, consulte [Limites de permissões](#) na IAM documentação.

informações de identificação pessoal () PII

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

PII

Veja 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](#).

PLM

Veja o gerenciamento [do ciclo de vida do produto](#).

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pressão de predicados

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

controle preventivo

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

principal (entidade principal)

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

Privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto () PLM

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

ambiente de produção

Veja o [ambiente](#).

controlador lógico programável () PLC

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

pseudonimização

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

publicar/assinar (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

RACImatriz

Veja [responsável, responsável, consultado, informado \(\) RACI](#).

ransomware

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

RASCImatriz

Veja [responsável, responsável, consultado, informado \(\) RACI](#).

RCAC

Veja o [controle de acesso por linha e coluna](#).

réplica de leitura

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

rearquiteta

Veja [7 Rs](#).

objetivo do ponto de recuperação (RPO)

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja [7 Rs](#).

Região

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

regressão

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

redefinir a hospedagem

Veja [7 Rs](#).

versão

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

realocar

Veja [7 Rs](#).

redefinir a plataforma

Veja [7 Rs](#).

recomprar

Veja [7 Rs](#).

resiliência

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

política baseada em recurso

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

matriz responsável, responsável, consultada, informada () RACI

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

controle responsivo

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

reter

Veja [7 Rs](#).

aposentar-se

Veja [7 Rs](#).

rotação

O processo de atualizar periodicamente um [segredo](#) para dificultar o acesso das credenciais por um invasor.

controle de acesso por linha e coluna (RCAC)

O uso de SQL expressões básicas e flexíveis que tenham regras de acesso definidas. 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

SAML2.0

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

SCADA

Veja [controle de supervisão e aquisição de dados](#).

SCP

Veja a [política de controle de serviços](#).

secret

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

controle de segurança

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

fortalecimento da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviço (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização no AWS Organizations. SCPs define barreiras ou estabeleça limites nas ações que um administrador pode delegar a usuários ou funções. Você pode usar SCPs como listas de permissão ou listas de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte [Políticas de controle de serviço](#) na AWS Organizations documentação.

service endpoint (endpoint de serviço)

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

contrato de nível de serviço () SLA

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

indicador de nível de serviço () SLI

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

objetivo de nível de serviço () SLO

Uma métrica alvo que representa a integridade de um serviço, conforme medida por um indicador de [nível de serviço](#).

modelo de responsabilidade compartilhada

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

SIEM

Veja [informações de segurança e sistema de gerenciamento de eventos](#).

ponto único de falha (SPOF)

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

SLA

Veja o contrato [de nível de serviço](#).

SLI

Veja o indicador [de nível de serviço](#).

SLO

Veja o objetivo do [nível de serviço](#).

split-and-seed modelo

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

SPOF

Veja [um único ponto de falha](#).

esquema de estrelas

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

padrão strangler fig

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

sub-rede

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

controle de supervisão e aquisição de dados () SCADA

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o [ambiente](#).

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o [ambiente](#).

V

aspiração

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

controle de versões

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

VPCespiando

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

WORM

Veja [escrever uma vez, ler muitas](#).

WQF

Consulte [Estrutura de qualificação AWS da carga de](#) trabalho.

escreva uma vez, leia muitos (WORM)

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

Z

exploração de dia zero

Um ataque, geralmente malware, que tira proveito de uma vulnerabilidade de [dia zero](#).

vulnerabilidade de dia zero

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

aplicação zumbi

Um aplicativo que tem uma média CPU e um uso de memória abaixo de 5%. Em um projeto de migração, é comum retirar essas aplicações.

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