



Implementando controles de segurança em AWS

AWS Orientação prescritiva



AWS Orientação prescritiva: Implementando controles de segurança em 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 desprestigie a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

Introdução	1
Público-alvo	1
Resultados de negócios desejados	3
Controles de segurança na estrutura de governança	4
Tipos de controles de segurança	6
Controles preventivos	6
Objetivos	7
Processar	8
Casos de uso	8
Tecnologia	9
Resultados de negócios	10
Controles proativos	11
Objetivos	11
Processar	12
Casos de uso	12
Tecnologia	13
Resultados de negócios	13
Controles detectivos	14
Objetivos	15
Processar	15
Casos de uso	15
Tecnologia	16
Resultados de negócios	19
Controles responsivos	19
Objetivos	20
Processar	20
Casos de uso	21
Tecnologia	21
Resultados de negócios	21
Próximas etapas	22
Perguntas frequentes	23
Em que devo me concentrar se eu tiver tempo e recursos limitados e não conseguir implementar todos esses tipos de controle?	23
Recursos	24

Documentação AWS	24
Publicações no blog da AWS	24
Outros recursos	24
Histórico do documento	25
Glossário	26
#	26
A	27
B	30
C	32
D	35
E	39
F	41
G	43
H	43
I	45
L	47
M	48
O	52
P	55
Q	58
R	58
S	61
T	65
U	66
V	67
W	67
Z	68
.....	lxx

Implementar controles de segurança na AWS

Iqbal Umair, Gurpreet Kaur Cheema, Wasim Hossain, Joseph Nguyen, San Brar e Lucia Vanta, Amazon Web Services (AWS)

Dezembro de 2023 ([histórico do documento](#))

A segurança é fundamental para todas as empresas e é um pilar fundamental na AWS Well-Architected Framework. No entanto, muitos não sabem como lidar com as considerações de segurança e criar uma estratégia holística automatizada de testes e remediação de segurança para seus ambientes de nuvem. Ao usar ferramentas e Serviços da AWS, como o AWS Config, o Amazon GuardDuty e o AWS CloudFormation, é possível criar uma estratégia de teste de segurança e incorporá-la aos seus ambientes da Nuvem AWS.

Para ajudar a cumprir a política e os padrões de segurança da sua empresa, controles de segurança são as barreiras de proteção técnicas ou administrativas que ajudam a prevenir, detectar ou reduzir a capacidade de um agente de ameaça explorar uma vulnerabilidade de segurança. Eles são projetados para proteger a confidencialidade, a integridade e a disponibilidade de recursos e dados. Veja a seguir exemplos de controles de segurança:

- Implementar a autenticação multifatorial para usuários que precisam fazer login em uma aplicação
- Ações de registro, monitoramento e consulta com o objetivo de realizar auditorias em tempo real da atividade da conta
- Garantir que dados confidenciais sejam criptografados
- Garantir que os logs sejam armazenados de acordo com a política de retenção da empresa

Existem quatro tipos de controles de segurança: preventivos, proativos, detectivos e responsivos. Este guia descreve cada tipo em mais detalhes e se concentra em como implementar e automatizar esses controles na Nuvem AWS. Este guia ajuda você a implementar controles de segurança contínuos e proativos.

Público-alvo

Este guia é voltado para arquitetos e engenheiros de segurança responsáveis pela implementação de controles de segurança na Nuvem AWS. Se sua empresa não tiver definido uma política de segurança, objetivos de controle ou padrões, conforme descrito no [Controles de segurança na](#)

[estrutura de governança](#), recomendamos que você conclua essas tarefas de governança antes de continuar com este guia.

Resultados de negócios desejados

As empresas usam controles de segurança para mitigar ou atuara como defesas contra riscos em seus sistemas de TI. Os controles definem a linha de base dos requisitos para satisfazer os principais objetivos de segurança de um programa de TI e sua estratégia de segurança. Ter controles implementados melhora a postura de segurança de uma empresa, protegendo a confidencialidade, integridade e disponibilidade dos dados e ativos de TI. Sem os controles, seria difícil saber onde é necessário focar e investir para estabelecer uma linha de base de segurança.

Os controles de segurança podem ser usados para lidar com uma variedade de cenários. Os exemplos incluem atender aos requisitos decorrentes de avaliações de risco, alcançar os padrões do setor ou cumprir as regulamentações. A satisfação dos controles de segurança demonstra que você mediu o risco de um sistema, determinou o nível de proteção necessário e implementou soluções proativamente. Fatores adicionais, como negócios, setor e geografia, podem ditar os controles de segurança de que você precisa.

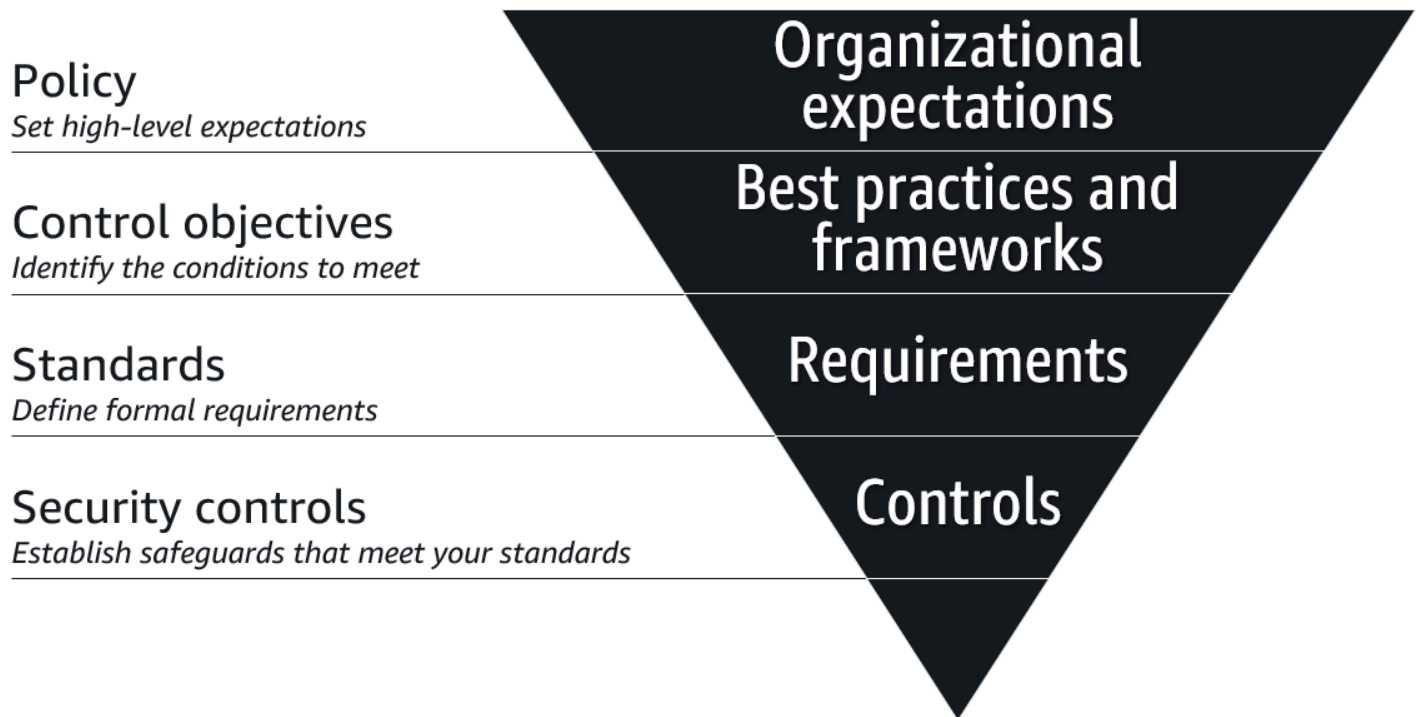
Veja a seguir alguns casos de uso comuns para a implementação de controles de segurança:

- Uma avaliação de segurança de uma aplicação identificou a necessidade de controles de acesso com base na confidencialidade dos dados que estão sendo processados.
- Você deve cumprir os padrões de segurança, como o Payment Card Industry Data Security Standard (PCI DSS), o HIPAA (Health Insurance Portability and Accountability Act) ou o National Institute of Standards and Technology (NIST).
- Você precisa proteger informações confidenciais para transações comerciais.
- Sua empresa se expandiu para uma região geográfica que exige controles de segurança, como uma região que exige conformidade com o Regulamento Geral de Proteção de Dados (GDPR).

Depois de ler este guia, você estará familiarizado com os quatro tipos de controles de segurança, entenderá como eles fazem parte de sua estrutura de governança de segurança e estará preparado para começar a implementar e automatizar os controles de segurança na Nuvem AWS.

Controles de segurança na estrutura de governança

É importante planejar a partir de um nível básico. Como começar? A figura a seguir mostra como você pode criar uma estratégia de governança de segurança com base em uma política, objetivos de controle, padrões e controles de segurança.



A seguir estão os componentes hierárquicos de uma estratégia de governança para segurança:

- **Política** – Uma política é a base de qualquer estratégia de governança de segurança cibernética. É um documento que declara as expectativas da empresa, como obrigações legais, regulatórias ou contratuais que ela deve cumprir. As políticas podem variar de acordo com o setor e a região.
- **Objetivos de controle** – Objetivos de controle são metas, como as práticas recomendadas reconhecidas pelo setor, que ajudam você a cumprir a intenção de uma política. Para computação em nuvem, muitas empresas adotam a [Matriz de controles de nuvem \(CCM\)](#) (site da Cloud Security Alliance), que é uma estrutura de objetivos de controle de segurança cibernética.
- **Padrões** – Padrões são requisitos formalmente estabelecidos que satisfazem um objetivo de controle. Os padrões podem incluir processos, ações ou configurações e são quantificáveis para que você possa medir a performance em relação ao padrão.
- **Controles de segurança** – Controles de segurança são os mecanismos técnicos ou administrativos que você implementou para implementar os padrões. Todos os controles de segurança são

mapeados para padrões, mas nem todos padrões são mapeados para controles de segurança. O teste dos controles de segurança foi projetado para monitorar e medir se você está efetivamente cumprindo os padrões definidos.

Este guia se concentra em como projetar e implementar tipos comuns de controles de segurança na Nuvem AWS.

Tipos de controles de segurança

Há quatro tipos principais de controles de segurança:

- [Controles preventivos](#): controles desenvolvidos para evitar que um evento ocorra.
- [Controles proativos](#): controles desenvolvidos para evitar a criação de recursos fora de conformidade.
- [Controles detectivos](#): controles desenvolvidos para detectar, registrar e alertar após a ocorrência de um evento.
- [Controles responsivos](#): controles desenvolvidos para impulsionar a remediação de eventos adversos ou desvios de sua linha de base de segurança.

Uma estratégia de segurança eficaz inclui todos os quatro tipos de controles de segurança. Embora os controles preventivos sejam a primeira linha de defesa para ajudar a impedir acesso não autorizado ou alterações indesejadas em sua rede, é importante garantir que você estabeleça controles de detecção e responsivos para saber quando um evento ocorrer e conseguir tomar as medidas imediatas e apropriadas para corrigi-lo. O uso de controles proativos adiciona outra camada de segurança porque complementa os controles preventivos, que geralmente são de natureza mais rígida.

As seções a seguir descrevem cada tipo de controle em mais detalhes. Elas abordam os objetivos, o processo de implementação, os casos de uso, as considerações tecnológicas e os resultados desejados de cada tipo de controle.

Controles preventivos

Controles preventivos são controles de segurança projetados para evitar que um evento ocorra. Essas barreiras de proteção são a primeira linha de defesa para ajudar a evitar acesso não autorizado ou alterações indesejadas em sua rede. Um exemplo de controle preventivo é uma função AWS Identity and Access Management (IAM) que tem acesso somente para leitura porque ajuda a evitar ações de gravação não intencionais de usuários não autorizados.

Analise o seguinte sobre esse tipo de controle:

- [Objetivos](#)
- [Processar](#)

- [Casos de uso](#)
- [Tecnologia](#)
- [Resultados de negócios](#)

Objetivos

O objetivo principal dos controles preventivos é minimizar ou evitar a probabilidade de ocorrência de um evento de ameaça. O controle deve ajudar a impedir acesso não autorizado ao sistema e evitar que alterações não intencionais afetem o sistema. A seguir estão os objetivos dos controles preventivos:

- Segregação de tarefas – Os controles preventivos podem estabelecer limites lógicos que restringem privilégios, autorizando que as permissões executem somente tarefas específicas em contas ou ambientes designados. Os exemplos incluem:
 - Segmentar workloads em contas diferentes para serviços específicos
 - Separar e contas em ambientes isolados de produção, desenvolvimento e teste
 - Delegar acesso e responsabilidades a várias entidades para realizar funções específicas, como usar perfis do IAM ou perfis assumidos para permitir que somente funções de trabalho específicas realizem determinadas ações
- Controle de acesso – Controles preventivos podem conceder ou negar de forma consistente acesso a recursos e dados no ambiente. Os exemplos incluem:
 - Impedir que os usuários excedam as permissões pretendidas, conhecidas como escalonamento de privilégios
 - Restringir acesso a aplicações e dados somente a usuários e serviços autorizados
 - Manter pequeno o grupo de administradores
 - Evitar usar as credenciais do usuário raiz
- Imposição – Os controles preventivos podem ajudar sua empresa a aderir às suas políticas, diretrizes e padrões. Os exemplos incluem:
 - Configurações de bloqueio que servem como linha de base de segurança mínima
 - Implementar medidas de segurança adicionais, como autenticação multifatorial
 - Evitar tarefas e ações não padrão que são executadas por perfis não aprovados

Processar

Mapeamento de controle preventivo é o processo de mapear controles em requisitos e usar políticas para implementar esses controles restringindo, desativando ou bloqueando. Ao mapear controles, considere o efeito proativo que eles têm no ambiente, nos recursos e nos usuários. A seguir estão as práticas recomendadas para mapear controles:

- Controles rígidos que proíbem uma atividade devem ser mapeados para ambientes de produção em que a ação exija processos de revisão, aprovação e mudança.
- Ambientes de desenvolvimento ou contidos podem ter menos controles preventivos para fornecer a agilidade de criar e testar.
- A classificação de dados, o nível de risco de um ativo e a política de gerenciamento de riscos ditam os controles preventivos.
- Mapeie as estruturas existentes como evidência de conformidade com padrões e regulamentações.
- Implemente controles preventivos por localização geográfica, ambiente, contas, redes, usuários, perfis ou recursos.

Casos de uso

Tratamento de tags

Um perfil que pode acessar todos os dados em uma conta é criada. Se houver dados confidenciais e criptografados, privilégios excessivamente permissivos poderão representar um risco, dependendo dos usuários ou grupos que possam assumir o perfil. Ao usar uma política de chaves em AWS Key Management Service (AWS KMS), você pode controlar quem tem acesso à chave e decifrar os dados.

Escalonamento de privilégios

Se permissões administrativas e de gravação forem atribuídas de forma muito ampla, um usuário poderá contornar os limites das permissões pretendidas e conceder a si mesmo privilégios adicionais. O usuário que cria e gerencia um perfil pode atribuir um limite de permissões, que define os privilégios máximos permitidos para o perfil.

Bloqueio da workload

Se sua empresa não tiver uma necessidade previsível de usar serviços específicos, habilite uma política de controle de serviços que limite quais serviços podem operar nas contas dos membros de uma organização ou restrinja os serviços com base no. Região da AWS Esse controle preventivo pode reduzir o escopo do impacto se um agente de ameaça conseguir comprometer e acessar uma conta em sua organização. Para obter mais informações, consulte [Políticas de controle de serviço](#) neste guia.

Impacto em outras aplicações

Os controles preventivos podem impor o uso de serviços e recursos, como IAM, criptografia e registro, a fim de atender aos requisitos de segurança de suas aplicações. Você também pode usar esses controles para ajudar a se proteger contra vulnerabilidades, limitando as ações que um agente de ameaças pode explorar devido a erros não intencionais ou configuração incorreta.

Tecnologia

Políticas de controle de serviço

Em AWS Organizations, [as políticas de controle de serviços](#) (SCPs) definem o máximo de permissões disponíveis para contas de membros em uma organização. Essas políticas ajudam as contas a se manterem dentro das diretrizes de controle de acesso da organização. Observe o seguinte ao projetar SCPs para sua organização:

- Os SCPs são controles preventivos porque definem e impõem as permissões máximas permitidas para funções e usuários do IAM nas contas dos membros da organização.
- Os SCPs afetam somente as funções e os usuários do IAM nas contas dos membros da organização. Isso não afeta os usuários e os perfis na conta de gerenciamento da organização.

Você pode tornar um SCP mais granular definindo as permissões máximas para cada Região da AWS.

Limites de permissões do IAM

Em AWS Identity and Access Management (IAM), um [limite de permissões](#) é usado para definir o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuários ou funções). O limite de permissões de uma entidade permite que ela execute

somente as ações permitidas por ambas as políticas baseadas em identidade e seus limites de permissões. Observe o seguinte ao usar limites de permissões:

- Você pode usar uma política AWS gerenciada ou uma política gerenciada pelo cliente para definir o limite de uma entidade do IAM.
- Um limite de permissões não concede permissões por si só. A política de limite de permissões restringe as permissões concedidas à entidade do IAM.

Resultados de negócios

Economia de tempo

- Ao adicionar automação depois de configurar os controles preventivos, você poderá reduzir a necessidade de intervenção manual e a frequência de erros.
- Usar limites de permissão como controle preventivo ajuda as equipes de segurança e IAM a se concentrarem em tarefas críticas, como governança e suporte.

Conformidade regulatória

- Talvez as empresas precisem cumprir as regulamentações internas ou do setor. Essas podem ser restrições regionais, restrições de usuários e perfis ou restrições de serviço. Os SCPs podem ajudar você a manter a conformidade e evitar penalidades por violação.

Redução de risco

- Com o crescimento, o número de solicitações para criar e gerenciar novos perfis e políticas aumenta. Torna-se mais difícil entender o contexto do que é necessário para criar manualmente as permissões para cada aplicação. O estabelecimento de controles preventivos funciona como uma linha de base e ajuda a impedir que os usuários realizem ações não intencionais, mesmo que tenham acesso acidental.
- A aplicação de controles preventivos às políticas de acesso fornece uma camada adicional para ajudar a proteger dados e ativos.

Controles proativos

Controles proativos são controles de segurança projetados para evitar a criação de recursos fora de conformidade. Esses controles podem reduzir o número de eventos de segurança tratados por controles responsivos e detectivos. Esses controles garantem que os recursos implantados estejam em conformidade antes de serem implantados. Portanto, não há nenhum evento de detecção que exija resposta ou remediação.

Por exemplo, você poderia ter um controle detectivo que notificasse você se um bucket do Amazon Simple Storage Service (Amazon S3) se tornasse acessível ao público. Você também pode ter um controle responsivo que corrija isso. Embora você já tenha esses dois controles em vigor, é possível acrescentar outra camada de proteção adicionando um controle proativo. Por meio AWS CloudFormation disso, o controle proativo pode impedir a criação de atualização de qualquer bucket do S3 que tenha acesso público habilitado. Os agentes da ameaça ainda podem contornar esse controle e implantar ou modificar recursos externos. CloudFormation Nesse caso, os controles detectivos e responsivos corrigiriam o evento de segurança.

Analise o seguinte sobre esse tipo de controle:

- [Objetivos](#)
- [Processar](#)
- [Casos de uso](#)
- [Tecnologia](#)
- [Resultados de negócios](#)

Objetivos

- Os controles proativos ajudam você a melhorar operações de segurança e processos de qualidade.
- Os controles proativos podem ajudar você a respeitar políticas, padrões e obrigações regulatórias ou de conformidade de segurança.
- Os controles proativos podem impedir a criação de recursos fora de conformidade.
- Os controles proativos podem reduzir o número de descobertas de segurança.
- Os controles proativos fornecem outra camada de proteção contra agentes de ameaças que ignoram os controles preventivos e tentam implantar recursos fora de conformidade.

- Em combinação com controles preventivos, detectivos e responsivos, os controles proativos podem ajudá-lo a lidar com incidentes de segurança potenciais.

Processar

Os controles proativos complementam os controles preventivos. Os controles proativos reduzem os riscos de segurança da sua organização e reforçam a implantação de recursos compatíveis. Esses controles avaliam a conformidade do recurso antes que ele seja criado ou atualizado. Os controles proativos geralmente são implementados usando CloudFormation ganchos. Se o recurso falhar na validação do controle proativo, você poderá optar por reprovar a implantação do recurso ou apresentar uma mensagem de aviso. A seguir são apresentadas algumas dicas e práticas recomendadas para criar controles proativos:

- Certifique-se de que os controles proativos sejam mapeados de acordo com os requisitos de conformidade da sua organização.
- Certifique-se de que os controles proativos sigam as práticas recomendadas de segurança para o serviço associado.
- Use CloudFormation StackSets nossa outra solução para implantar controles proativos em várias Regiões da AWS contas.
- Certifique-se de que a mensagem de aviso ou falha associada a um controle proativo seja explícita e clara. Isso ajuda os desenvolvedores a entender o motivo pelo qual o recurso não foi aprovado na avaliação.
- Ao criar novos controles proativos, comece no modo de observação. Isso significa que você envia uma mensagem de aviso em vez de reprovar a implantação do recurso. Isso ajuda a compreender o impacto do controle proativo.
- Habilite o login no Amazon CloudWatch Logs para controles proativos.
- Se você precisar monitorar a invocação de um controle proativo específico, use uma EventBridge regra da Amazon e assine os eventos de invocação do gancho. CloudFormation

Casos de uso

- Impeça a implantação de recursos fora de conformidade
- Atenda a requisitos de conformidade
- Melhore a qualidade do código exigindo a correção de problemas de segurança antes da implantação

- Reduza o tempo de inatividade operacional associado à correção de problemas de segurança após a implantação

Tecnologia

CloudFormation ganchos

[AWS CloudFormation](#) ajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.

[CloudFormation hooks](#) avaliam proativamente a configuração de seus CloudFormation recursos antes de serem implantados. Se recursos fora de conformidade forem encontrados, ele retornará um status de falha. Com base no modo de falha do gancho, CloudFormation pode falhar a operação ou apresentar um aviso que permita ao usuário continuar com a implantação. Você pode usar os hooks disponíveis ou desenvolver os seus próprios.

AWS Control Tower

[AWS Control Tower](#) ajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas prescritivas. AWS Control Tower oferece [controles proativos](#) pré-configurados que você pode ativar em sua landing zone. Se sua landing zone estiver configurada usando AWS Control Tower, você pode usar esses controles proativos opcionais como ponto de partida para sua organização. Você pode criar controles proativos adicionais e personalizados CloudFormation conforme necessário.

Resultados de negócios

Menos esforço humano e menos erros

Os controles proativos reduzem os riscos de erros humanos que levam à implantação de recursos fora de conformidade. Eles também reduzem o esforço humano mais à frente no ciclo de desenvolvimento porque fazem com que os desenvolvedores considerem a segurança dos recursos antes da implantação. Isso aplica a prática de mudança à esquerda à criação de recursos seguros, pois força a conformidade no início do ciclo de vida do desenvolvimento.

Custos reduzidos

Geralmente, é mais caro corrigir um problema de segurança após a implantação. Identificar e corrigir problemas no início do ciclo de desenvolvimento reduz o custo do desenvolvimento.

Economia de tempo

Como os controles proativos evitam a implantação de recursos fora de conformidade, eles reduzem o tempo gasto na triagem e na correção de problemas de segurança. Eles também indicam o número de descobertas de segurança que os controles detectivos identificariam posteriormente no ciclo de desenvolvimento.

Conformidade regulatória

Se sua organização precisa atender a regulamentações internas ou do setor, controles proativos podem ajudar você a manter a conformidade e evitar penalidades por violações.

Redução de risco

Os controles proativos ajudam os desenvolvedores a implantar recursos em conformidade e criados com mais segurança. Assim, os controles proativos reduzem os riscos de segurança da sua organização.

Controles detectivos

Controles detectivos são controles de segurança projetados para detectar, registrar e alertar após a ocorrência de um evento. Os controles detectivos são uma parte fundamental das estruturas de governança. Essas barreiras de proteção são uma segunda linha de defesa, notificando você sobre problemas de segurança que contornaram os controles preventivos.

Por exemplo, você pode aplicar um controle detectivo que detecte e notifique você se um bucket do Amazon Simple Storage Service (Amazon S3) se tornar acessível ao público. Embora você possa ter controles preventivos que desabilitem o acesso público aos buckets do S3 no nível da conta e, em seguida, desabilitem o acesso por meio de SCPs, um agente de ameaças pode contornar esses controles preventivos fazendo login como usuário administrativo. Nessas situações, um controle detectivo pode alertar você sobre a configuração incorreta e a possível ameaça.

Analise o seguinte sobre esse tipo de controle:

- [Objetivos](#)
- [Processar](#)
- [Casos de uso](#)
- [Tecnologia](#)

- [Resultados de negócios](#)

Objetivos

- Os controles detectivos ajudam você a melhorar processos de operações de segurança e processos de qualidade.
- Os controles detectivos ajudam você a cumprir obrigações regulatórias, legais ou de conformidade.
- Os controles detectivos fornecem às equipes de operações de segurança visibilidade para responder aos problemas de segurança, incluindo ameaças avançadas que contornem os controles preventivos.
- Os controles detectivos podem ajudar você a identificar a resposta adequada a problemas de segurança e possíveis ameaças.

Processar

Você implementa controles detectivos em duas fases. Primeiro, você configura o sistema para registrar eventos e estados de recursos em um local centralizado, como o Amazon CloudWatch Logs. Depois que o registro centralizado estiver em vigor, você analisará esses logs para detectar anomalias que possam indicar uma ameaça. Cada análise é um controle que é mapeado de acordo com seus requisitos e políticas originais. Por exemplo, você pode criar um controle detectivo que pesquise um padrão específico nos logs e gere um alerta se houver correspondência. Os controles detectivos são usados pelas equipes de segurança para melhorar sua visibilidade geral das ameaças e riscos aos quais o sistema pode estar exposto.

Casos de uso

Detecção de comportamento suspeito

Os controles detectivos ajudam a identificar qualquer atividade anômala, como credenciais de usuário privilegiado comprometidas ou acesso ou exfiltração de dados confidenciais. Esses controles são fatores reativos importantes que podem ajudar sua empresa a identificar e entender o escopo da atividade anômala.

Detecção de fraudes

Esses controles ajudam a detectar e identificar uma ameaça dentro da sua empresa, como um usuário que está contornando políticas e realizando transações não autorizadas.

Conformidade

Os controles detectivos ajudam você a atender aos requisitos de conformidade, como o Payment Card Industry Data Security Standard (PCI DSS), e podem ajudar a evitar roubo de identidades. Esses controles podem ajudar você a descobrir e proteger informações confidenciais que estão sujeitas à conformidade regulatória, como informações de identificação pessoal.

Análise automatizada

Os controles detectivos podem analisar automaticamente logs para detectar anomalias e outros indicadores de atividades não autorizadas.

Você pode analisar automaticamente logs de diferentes fontes, como logs do AWS CloudTrail , [Log de fluxo de VPC](#), e logs do Sistema de Nomes de Domínio (DNS), em busca de indicações de atividades possivelmente mal-intencionadas. Para ajudar na organização, agregue alertas ou descobertas de segurança de vários Serviços da AWS locais em um local centralizado.

Tecnologia

Um controle detectivo comum é implementar um ou mais serviços de monitoramento, que podem analisar fontes de dados, como logs, para identificar ameaças à segurança. No Nuvem AWS, você pode analisar fontes como AWS CloudTrail registros, registros de acesso do Amazon S3 e registros de fluxo da Amazon Virtual Private Cloud para ajudar a detectar atividades incomuns. AWS serviços de segurança, como Amazon GuardDuty, Amazon Detective e Amazon Macie AWS Security Hub, têm funcionalidades de monitoramento integradas.

GuardDuty e o Security Hub

[A Amazon GuardDuty](#) usa inteligência de ameaças, aprendizado de máquina e técnicas de detecção de anomalias para monitorar continuamente suas fontes de log em busca de atividades maliciosas ou não autorizadas. O painel fornece informações sobre a integridade em tempo real de suas cargas de trabalho Contas da AWS e de suas cargas de trabalho. Você pode se integrar GuardDuty a [AWS Security Hub](#) um serviço de gerenciamento de postura de segurança na nuvem que verifica a adesão às melhores práticas, agrega alertas e permite a remediação automatizada. GuardDuty envia descobertas para o Security Hub como forma de centralizar as informações. Você pode integrar ainda mais o Security Hub às soluções de gerenciamento de eventos e informações de segurança (SIEM) para ampliar os recursos de monitoramento e alerta da sua organização.

Macie

O [Amazon Macie](#) é um serviço de segurança e privacidade de dados totalmente gerenciado que usa machine learning e correspondência de padrões para ajudar a descobrir e proteger dados confidenciais na AWS. A seguir estão alguns dos controles e recursos detectivos disponíveis no Macie:

- O Macie inspeciona o inventário de um bucket e todos os objetos armazenados no Amazon S3. Essas informações podem ser apresentadas em uma única visualização do painel, fornecendo visibilidade e ajudando você a avaliar a segurança do bucket.
- Para descobrir dados confidenciais, o Macie usa identificadores de dados gerenciados integrados e também oferece suporte a identificadores de dados personalizados.
- O Macie se integra nativamente com outras Serviços da AWS ferramentas. Por exemplo, Macie emite descobertas como EventBridge eventos da Amazon, que são enviadas automaticamente para o Security Hub.

A seguir estão as práticas recomendadas para configurar controles detectivos no Macie:

- Ative o Macie em todas as contas. Ao usar o recurso de gerenciamento delegado, habilite o Macie em várias contas usando o AWS Organizations.
- Use o Macie para avaliar a postura de segurança dos buckets do S3 em suas contas. Isso ajuda a evitar a perda de dados, fornecendo visibilidade da localização e do acesso aos dados. Para obter mais informações, consulte [Analisar sua postura de segurança do Amazon S3](#) (documentação do Macie).
- Automatize a descoberta de dados confidenciais em seus buckets do S3 executando e programando trabalhos automatizados de processamento e descoberta de dados. Isso inspeciona regularmente os buckets do S3 em busca de dados confidenciais.

AWS Config

[AWS Config](#) audita e registra a conformidade dos AWS recursos. AWS Config descobre AWS os recursos existentes e gera um inventário completo, junto com os detalhes de configuração de cada recurso. Se houver alguma alteração na configuração, ele registrará essas alterações e fornecerá uma notificação. Isso pode ajudar você a detectar e reverter alterações de infraestrutura não autorizadas. Você pode usar regras AWS gerenciadas e criar regras personalizadas.

A seguir estão as práticas recomendadas para configurar controles detectivos no AWS Config:

- Ative AWS Config para cada conta de membro na organização e para cada uma Região da AWS que contenha recursos que você deseja proteger.
- Configure os alertas do Amazon Simple Notification Service (Amazon SNS) para qualquer alteração de configuração.
- Armazene os dados de configuração em um bucket do S3 e use o Amazon Athena para analisá-los.
- Automatize a remediação de recursos não compatíveis usando [Automação](#), um recurso do AWS Systems Manager.
- Use EventBridge nosso Amazon SNS para configurar notificações sobre recursos não AWS compatíveis.

Trusted Advisor

[AWS Trusted Advisor](#) pode ser usado como um serviço para controles detectivos. Por meio de um conjunto de verificações, Trusted Advisor identifica áreas nas quais você pode otimizar sua infraestrutura, melhorar o desempenho e a segurança ou reduzir custos. Trusted Advisor fornece recomendações com base nas AWS melhores práticas que você pode seguir para melhorar seus serviços e recursos. Os planos Business e Enterprise Support fornecem acesso a todas as verificações disponíveis dos [pilares](#) do AWS Well-Architected Framework.

A seguir estão as práticas recomendadas para configurar controles detectivos no Trusted Advisor:

- Revisar o resumo do nível de verificação
- Implemente recomendações específicas de recursos para estados de aviso e erro.
- Verifique Trusted Advisor com frequência para revisar e implementar ativamente suas recomendações.

Amazon Inspector

O [Amazon Inspector](#) é um serviço automatizado de gerenciamento de vulnerabilidades que, após ser habilitado, verifica continuamente workloads em busca de vulnerabilidades de software e exposição não intencional da rede. Ele contextualiza as descobertas em uma pontuação de risco que pode ajudar você a determinar as próximas etapas, como corrigir ou confirmar o status de conformidade.

A seguir estão as práticas recomendadas para configurar controles detectivos no Amazon Inspector:

- Habilite o Amazon Inspector em todas as contas e integre-o EventBridge ao Security Hub para configurar relatórios e notificações para vulnerabilidades de segurança.
- Priorize as remediações e outras ações com base na pontuação de risco do Amazon Inspector.

Resultados de negócios

Menos esforço humano e menos erros

Você pode atingir automação usando a infraestrutura como código (IaC). Automatizar implantação, configuração de serviços e ferramentas de monitoramento e remediação reduz o risco de erros manuais e reduz a quantidade de tempo e esforço necessários para escalar esses controles detectivos. A automação ajuda no desenvolvimento de runbooks de segurança e reduz as operações manuais para analistas de segurança. Revisões regulares ajudam a ajustar as ferramentas de automação e a iterar e melhorar continuamente os controles detectivos.

Ações apropriadas contra possíveis ameaças

Capturar e analisar eventos a partir de logs e métricas é crucial para ganhar visibilidade. Isso ajuda os analistas a agir sobre eventos de segurança e possíveis ameaças para ajudar a proteger suas workloads. A capacidade de identificar rapidamente quais vulnerabilidades existem ajuda os analistas a tomarem as medidas apropriadas para resolvê-las e corrigi-las.

Melhor resposta a incidentes e tratamento investigativo

A automação das ferramentas de controle detectivas pode aumentar a velocidade de detecção, investigação e recuperação. Alertas e notificações automatizados com base em condições definidas permitem que os analistas de segurança investiguem e respondam adequadamente. Esses fatores responsivos podem ajudá-lo a identificar e entender o escopo da atividade anômala.

Controles responsivos

Controles responsivos são controles de segurança projetados para impulsionar a remediação de eventos adversos ou desvios de sua linha de base de segurança. Exemplos de controles técnicos responsivos incluem corrigir um sistema, colocar um vírus em quarentena, encerrar um processo ou reinicializar um sistema.

Analise o seguinte sobre esse tipo de controle:

- [Objetivos](#)
- [Processar](#)
- [Casos de uso](#)
- [Tecnologia](#)
- [Resultados de negócios](#)

Objetivos

- Os controles responsivos podem ajudar você a criar runbooks para tipos comuns de ataques, como phishing ou força bruta.
- Controles responsivos podem implementar respostas automatizadas para possíveis problemas de segurança.
- Os controles responsivos podem corrigir automaticamente ações não intencionais ou não aprovadas nos AWS recursos, como excluir buckets S3 não criptografados.
- Os controles responsivos podem ser orquestrados para trabalhar com controles preventivos e detectivos para criar uma abordagem holística e proativa para lidar com possíveis incidentes de segurança.

Processar

Os controles detectivos são um pré-requisito para estabelecer controles responsivos. Você deve ser capaz de detectar o problema de segurança antes de poder corrigi-lo. Em seguida, você pode estabelecer uma política ou resposta ao problema de segurança. Por exemplo, no caso de um ataque de força bruta, um processo de remediação seria implementado. Depois que o processo de remediação existir, ele poderá ser automatizado e executado como um script usando uma linguagem de programação, como um script de shell.

Considere se o controle responsivo pode interromper uma workload de produção existente. Por exemplo, se o controle de segurança detectivo for buckets do S3 não devem ser acessíveis ao público e a remediação for desativar acesso público ao Amazon S3, isso poderá ter implicações significativas para sua empresa e seus clientes. Se o bucket do S3 estiver servindo um site público, desativar o acesso público poderá causar uma interrupção. Os bancos de dados são um exemplo semelhante. Se um banco de dados não precisar ser acessível publicamente pela Internet, desativar o acesso público poderá afetar a conectividade com a aplicação.

Casos de uso

- Resposta automática aos eventos de segurança detectados
- Remediação automática de vulnerabilidades de segurança detectadas
- Controle de recuperação automatizado para reduzir o tempo de inatividade operacional

Tecnologia

Security Hub

[AWS Security Hub](#) envia automaticamente todas as novas descobertas e todas as atualizações das descobertas existentes EventBridge como eventos. Você também pode criar ações personalizadas que enviam descobertas selecionadas e resultados de insights para EventBridge. Você pode configurar EventBridge para responder a cada tipo de evento. O evento pode iniciar uma AWS Lambda função que executa a ação de remediação.

AWS Config

[AWS Config](#) usa regras para avaliar seus AWS recursos e ajuda a corrigir recursos não compatíveis. AWS Config aplica a remediação usando a [AWS Systems Manager automação](#). Nos documentos de automação, você define as ações que deseja realizar em recursos que são AWS Config determinados como não compatíveis. Depois de criar documentos de automação, você pode usá-los no Systems Manager por meio do AWS Management Console ou usando APIs. Você pode optar por corrigir manual ou automaticamente recursos não compatíveis.

Resultados de negócios

Minimizar perda de dados

Depois de um incidente de segurança cibernética, o uso de controles de segurança responsivos poderá ajudar a minimizar a perda de dados e os danos ao sistema ou à rede. Controles responsivos também podem ajudar a restaurar sistemas e processos de negócios críticos o mais rápido possível, aumentando a resiliência de suas workloads.

Reduzir custo

A automação reduz os custos associados aos recursos humanos porque os membros da equipe não precisam responder manualmente aos incidentes nem gerenciá-los de outra forma. case-by-case

Próximas etapas

Depois de ler este guia, você estará familiarizado com os quatro tipos de controles de segurança, entenderá como eles fazem parte de sua estrutura de governança de segurança e estará preparado para começar a implementar e automatizar os controles de segurança na Nuvem AWS. Para obter mais informações, recomendamos que você revise as referências incluídas na seção [Recursos](#).

Também recomendamos que você execute as próximas etapas para avaliar a segurança da sua infraestrutura de nuvem e comece a implementar controles de segurança:

1. Habilite e configure o AWS Security Hub. Como prática recomendada, habilite os controles de padrões disponíveis. Para obter mais informações, consulte [Padrões e controles de segurança](#) (documentação do Security Hub).
2. Habilite e configure o AWS Config. Para obter mais informações, consulte [Introdução](#) (documentação do AWS Config).
3. Usando o Serviços da AWS como Security Hub, o Amazon Macie, o AWS Config, o AWS Trusted Advisor e o Amazon Inspector, avalie sua organização e a infraestrutura de conta, identifique áreas que precisam ser melhoradas, revise e faça recomendações desses serviços. Use o recurso de verificação de segurança no Security Hub para gerar uma pontuação de segurança para um padrão de segurança. Para obter mais informações, consulte [Determinar as pontuações de segurança](#) (documentação do Security Hub).
4. Implemente controles de segurança preventivos, proativos, detectivos e responsivos com base nas melhorias identificadas.
5. Conduza uma avaliação de segurança de acompanhamento para avaliar a eficácia dos controles de segurança implementados. No Security Hub, determine se a pontuação de segurança melhorou. Faça iterações para melhorar ou adicionar novos controles de segurança.
6. Estabeleça uma cadência regular para realizar avaliações de segurança, como anualmente.

Perguntas frequentes

Em que devo me concentrar se eu tiver tempo e recursos limitados e não conseguir implementar todos esses tipos de controle?

Recomendamos implementar o AWS Security Hub. O Security Hub tem um conjunto de controles de segurança automatizados, chamado [padrão de Práticas Recomendadas de Segurança Básica da AWS](#) (documentação do Security Hub). Esse é um conjunto altamente organizado de práticas recomendadas de segurança gerenciado por especialistas em segurança da AWS. Você pode executar esses controles padrão continuamente, sempre que houver alterações nos recursos associados, ou periodicamente, em uma programação regular. Cada controle tem uma pontuação de severidade específica para ajudá-lo a priorizar seus esforços de remediação. Para obter mais informações, consulte [Executar verificações de segurança](#) (documentação do Security Hub). Se estiver usando o AWS Control Tower, você também poderá revisar e optar por ativar seus [controles](#) preventivos, detectivos e proativos.

Recursos

Documentação AWS

- [AWS Security Reference Architecture \(AWS SRA\)](#)
- [Perspectiva de segurança do AWS CAF](#)
- [Práticas recomendadas de segurança, identidade e conformidade](#)
- Resposta de segurança automatizada na AWS (AWS Solution)
 - [Página de destino da solução](#)
 - [Guia de implementação](#)

Publicações no blog da AWS

- [Guia de identidade – Controles preventivos com o AWS Identity – SCPs](#)
- [Como implementar uma política de controle de serviços \(SCP\) somente para leitura para contas no AWS Organizations](#)
- [Práticas recomendadas para Políticas de controle de serviços do AWS Organizations em um ambiente com várias contas](#)
- [Mantenha a conformidade usando as Políticas de controle de serviços e garanta que elas sejam sempre aplicadas](#)
- [Quando e onde usar os limites de permissões do IAM](#)
- [Mantenha proativamente os recursos seguros e em conformidade com hooks do AWS CloudFormation](#)

Outros recursos

- [Matriz de controles de nuvem \(CCM\)](#) (Aliança de segurança na nuvem)
- [Limites de permissões de exemplo](#) (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
Controles proativos	Adicionamos informações sobre controles proativos a este guia, incluindo a seção Controles proativos .	4 de dezembro de 2023
Publicação inicial	—	12 de dezembro 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 o 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 (Amazon RDS) 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 instância do EC2 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 função SQL que opera em um grupo de linhas e calcula um único valor de retorno para o grupo. Exemplos de funções agregadas incluem SUM e MAX

AI

Veja [inteligência artificial](#).

AIOps

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

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para 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 por atributo (ABAC)

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

fonte de dados autorizada

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

Availability Zone (zona de disponibilidade)

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

AWS Estrutura de adoção da nuvem (AWS CAF)

Uma estrutura de diretrizes e melhores práticas AWS para ajudar as organizações a desenvolver um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS O CAF organiza a orientação em seis áreas de foco chamadas perspectivas: negócios, pessoas, governança, plataforma, segurança e operações. As perspectivas de negócios, pessoas e governança têm como foco habilidades e processos de negócios; as perspectivas de plataforma, segurança e operações concentram-se em habilidades e processos técnicos. Por exemplo, a perspectiva das pessoas tem como alvo as partes interessadas que lidam com recursos humanos (RH), funções de pessoal e gerenciamento de pessoal. Nessa perspectiva, o AWS CAF fornece orientação para desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o [site da AWS CAF](#) e o [whitepaper da AWS CAF](#).

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

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS

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

B

bot ruim

Um [bot](#) destinado a perturbar ou causar danos a indivíduos ou organizações.

BCP

Veja o [planejamento de continuidade de negócios](#).

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

acesso em vidro quebrado

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

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

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

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

classificação

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

criptografia no lado do cliente

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

Centro de Excelência da Nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas 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 [postagens do CCoE 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: realizar investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma zona de pouso, definir um CCoE, estabelecer um modelo de operações)
- Migração: migrar aplicações individuais
- Reinvenção: otimizar produtos e serviços e inovar na nuvem

Esses estágios foram definidos por Stephen Orban na postagem do blog [The Journey Toward Cloud-First & the Stages of Adoption](#) no blog 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, os dados de um CMDB são usados no estágio de descoberta e análise do portfólio da migração.

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja [visão computacional](#).

D

dados em repouso

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

classificação de dados

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

desvio de dados

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

dados em trânsito

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

malha de dados

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

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

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

implantação

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

ambiente de desenvolvimento

Veja o [ambiente](#).

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Consulte [linguagem de manipulação de banco](#) de dados.

design orientado por domínio

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

DR

Veja a [recuperação de desastres](#).

detecção de deriva

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

DVSM

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

E

EDA

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

computação de borda

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

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o [endpoint do serviço](#).

serviço de endpoint

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

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

environment (ambiente)

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

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

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

epic

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

ERP

Consulte [planejamento de recursos corporativos](#).

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a [filial](#).

recursos

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

importância do recurso

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

transformação de recursos

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

FGAC

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

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

G

bloqueio geográfico

Veja as [restrições geográficas](#).

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

estratégia greenfield

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

barreira de proteção

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

H

HA

Veja a [alta disponibilidade](#).

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

Uma correção urgente para um problema crítico em um ambiente de produção. Devido à sua urgência, um hotfix geralmente é feito fora do fluxo de trabalho 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 hiper cuidados, a equipe de migração normalmente transfere a responsabilidade pelas aplicações para a equipe de operações de nuvem.

I

IaC

Veja a [infraestrutura como código](#).

Política baseada em identidade

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

aplicação ociosa

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

IloT

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

infraestrutura imutável

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

VPC de entrada (admissão)

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

migração incremental

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

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 das Coisas Industrial (IIoT)

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

VPC de inspeção

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

Internet das Coisas (IoT)

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

interpretabilidade

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

IoT

Consulte [Internet das Coisas](#).

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

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

ITSM

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

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

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

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja [7 Rs](#).

sistema little-endian

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

ambientes inferiores

Veja o [ambiente](#).

M

machine learning (ML)

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

ramificação principal

Veja a [filial](#).

malware

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

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

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte [Migration Acceleration Program](#).

mecanismo

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

conta-membro

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

MES

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

Transporte de telemetria de enfileiramento de mensagens (MQTT)

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

microsserviço

Um serviço pequeno e independente que se comunica por meio de APIs bem definidas e normalmente pertence a equipes pequenas e autônomas. Por exemplo, um sistema de seguradora pode incluir microsserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos

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

arquitetura de microserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microserviço. Esses microserviços se comunicam por meio de uma interface bem definida usando APIs leves. Cada microserviço 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 microserviços em AWS](#)

Programa de Aceleração da Migração (MAP)

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

migração em escala

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

fábrica de migração

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

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

A abordagem usada para migrar uma carga de trabalho para 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](#).

MAPA

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

MQTT

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

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

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

CARVALHO

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

OCM

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

migração offline

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

OI

Veja a [integração de operações](#).

OLA

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

migração online

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

OPC-UA

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

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

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (OT)

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

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

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

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

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

OU

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

NÃO

Veja a [tecnologia operacional](#).

VPC de saída (egresso)

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

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja [informações de identificação pessoal](#).

manual

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

PLC

Consulte [controlador lógico programável](#).

AMEIXA

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

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pressão de predicados

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

controle preventivo

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

principal (entidade principal)

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

Privacidade por design

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

zonas hospedadas privadas

Um contêiner que armazena informações sobre como você quer que o Amazon Route 53 responda a consultas ao DNS para um domínio e seus subdomínios dentro de uma ou mais VPCs. Para obter mais informações, consulte [Como trabalhar com zonas hospedadas privadas](#) na documentação do Route 53.

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja o [ambiente](#).

controlador lógico programável (PLC)

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

pseudonimização

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

publicar/assinar (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

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

ransomware

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

Matriz RASCI

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

RCAC

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

réplica de leitura

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

rearquiteta

Veja [7 Rs](#).

objetivo de ponto de recuperação (RPO).

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, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja [7 Rs](#).

aposentar-se

Veja [7 Rs](#).

rotação

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja o [objetivo do ponto de recuperação](#).

RTO

Veja o [objetivo do tempo de recuperação](#).

runbook

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

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login AWS Management Console ou chamar as operações da AWS API sem que você precise criar um usuário no IAM para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte [Sobre a federação baseada em SAML 2.0](#) na documentação do IAM.

SCADA

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

SCP

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

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele consiste no valor secreto

e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte [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 sistema SIEM coleta, monitora e analisa dados de servidores, redes, dispositivos e outras fontes para detectar ameaças e violações de segurança e gerar alertas.

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

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

ponto único de falha (SPOF)

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

SLA

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

ESGUIO

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

SLO

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

split-and-seed modelo

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

CUSPE

Veja [um único ponto de falha](#).

esquema de estrelas

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

padrão strangler fig

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

sub-rede

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

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o [ambiente](#).

treinamento

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

gateway de trânsito

Um hub de trânsito de rede que pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações, consulte [O que é um gateway de trânsito](#) na AWS Transit Gateway documentação.

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o [ambiente](#).

V

aspiração

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

controle de versões

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

emparelhamento de VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

MINHOCA

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

WQF

Consulte o [AWS Workload Qualification Framework](#).

escreva uma vez, leia muitas (WORM)

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

Z

exploração de dia zero

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

vulnerabilidade de dia zero

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

aplicação zumbi

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

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