



Controles de segurança recomendados para implementar os recursos de segurança AWS do CAF

AWS Orientação prescritiva



AWS Orientação prescritiva: Controles de segurança recomendados para implementar os recursos de segurança AWS do CAF

Copyright © 2025 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 pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

Introdução	1
Controles de identidade e acesso	3
Atividade do usuário root	3
Chaves de acesso para o usuário root	4
MFA para o usuário-raiz	4
Práticas recomendadas do IAM	5
Privilégio mínimo	5
Guardrails no nível da carga de trabalho	6
Gire as chaves de acesso do IAM	7
Recursos compartilhados externamente	7
Controles de registro e monitoramento	8
CloudTrail Trilha multirregional	8
Registro de serviços e aplicativos	9
Registro centralizado	9
Acesso aos arquivos CloudTrail de log	10
Alertas para grupos de segurança ou alterações de ACL de rede	10
Alertas para CloudWatch alarmes	11
Controles de infraestrutura	12
CloudFront objetos raiz padrão	12
Digitalize o código do aplicativo	13
Crie camadas de rede	13
Use somente portas autorizadas	14
Acesso público aos documentos do Systems Manager	14
Acesso público às funções do Lambda	15
Atualizar grupo de segurança padrão	15
Verifique as vulnerabilidades e a exposição da rede	16
Configurar AWS WAF	17
Proteções avançadas contra ataques DDo S	17
Controlar o tráfego de rede	18
Controles de dados	19
Classifique os dados no nível da carga de trabalho	19
Estabeleça controles para cada nível de classificação de dados	20
Criptografe dados em repouso	21
Criptografe dados em trânsito	21

Acesso público aos snapshots do Amazon EBS	22
Acesso público aos snapshots do Amazon RDS	23
Acesso público ao Amazon RDS, Amazon Redshift e recursos AWS DMS	23
Acesso público aos buckets do S3	24
Exigir MFA para excluir dados do bucket do S3	25
OpenSearch Domínios de serviço em VPCs	25
Alertas para exclusão da chave KMS	26
Acesso público às chaves KMS	26
Os ouvintes usam protocolos seguros	27
Recomendações de resposta a incidentes	28
Plano de resposta a incidentes	28
Livros de corrida e manuais	29
Automação orientada por eventos	29
Suporte processo	30
Alertas para eventos de segurança	31
Próximas etapas	32
Histórico do documento	33
Glossário	34
#	34
A	35
B	38
C	40
D	43
E	48
F	50
G	52
H	53
eu	54
L	57
M	58
O	62
P	65
Q	68
R	68
S	72
T	76

U	77
V	78
W	78
Z	79
.....	lxxi

Controles de segurança recomendados para implementar os recursos de segurança AWS do CAF

Rishi Singla e Rován Omar, da Amazon Web Services (AWS)

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

A segurança é a principal prioridade em AWS. Para ajudar a aliviar sua carga operacional, você [compartilha a responsabilidade pela](#) segurança e conformidade da nuvem com AWS. AWS é responsável pela segurança da nuvem, o que significa proteger a infraestrutura que executa os serviços oferecidos no Nuvem AWS. Você é responsável pela segurança na nuvem, como seus dados e aplicativos. Este guia fornece [controles de segurança](#) que podem ajudá-lo a cumprir suas responsabilidades de segurança no Nuvem AWS.

O [AWS Cloud Adoption Framework \(AWS CAF\)](#) fornece as melhores práticas projetadas para melhorar sua prontidão para a nuvem. O AWS CAF categoriza essas melhores práticas em seis perspectivas: negócios, pessoas, governança, plataforma, segurança e operações. Este guia se concentra nos seguintes recursos na perspectiva da segurança:

- Gerenciamento de identidade e acesso — gerencie identidades humanas e de máquinas e suas permissões em grande escala.
- Detecção de ameaças — configure o registro e o monitoramento para detectar e investigar uma possível configuração incorreta de segurança, ameaça ou comportamento inesperado.
- Proteção da infraestrutura — Proteja sistemas e serviços contra acesso não intencional ou não autorizado e possíveis vulnerabilidades.
- Proteção de dados — categorize os dados com base nos níveis de sensibilidade. Mantenha a visibilidade e o controle sobre os dados e como eles são acessados e usados em sua organização.
- Resposta a incidentes — Estabeleça mecanismos para responder e mitigar o impacto potencial dos incidentes de segurança.

A falha na implementação de controles de segurança preventivos, detectivos e responsivos para esses recursos de segurança do AWS CAF pode representar um risco crítico para seu ambiente de nuvem e pode atrapalhar seus negócios. A implementação dos controles de segurança neste guia pode ajudar sua organização a proteger seu ambiente de nuvem.

Note

AWS fornece serviços, ferramentas e estruturas que podem ajudá-lo a operar com segurança no. Nuvem AWS Este guia se alinha e complementa o [AWS Well-Architected Framework AWS](#) , o [Cloud Adoption Framework AWS \(CAF\)](#), AWS a [Security Reference Architecture AWS \(SRA\)](#) e outras recomendações de segurança publicadas pela. AWS Os controles deste guia não abrangem todas as considerações de segurança na nuvem, e este guia não se destina a substituir essas estruturas.

Recomendações de controle de segurança para gerenciar identidade e acesso

Você pode criar identidades em AWS ou conectar uma fonte de identidade externa. Por meio de políticas AWS Identity and Access Management (IAM), você concede aos usuários as permissões necessárias para que eles possam acessar ou gerenciar AWS recursos e aplicativos integrados. O gerenciamento eficaz de identidade e acesso ajuda a validar se as pessoas e as máquinas certas têm acesso aos recursos certos sob as condições certas. O AWS Well-Architected Framework [fornece as melhores práticas para gerenciar identidades](#) e suas permissões. Exemplos de melhores práticas incluem confiar em um provedor de identidade centralizado e usar mecanismos de login robustos, como a autenticação multifator (MFA). Os controles de segurança nesta seção podem ajudá-lo a implementar essas melhores práticas.

Controles nesta seção:

- [Monitore e configure notificações para a atividade do usuário root](#)
- [Não crie chaves de acesso para o usuário-raiz](#)
- [Ativar o MFA para o usuário raiz](#)
- [Siga as melhores práticas de segurança do IAM](#)
- [Conceda permissões com privilégios mínimos](#)
- [Defina barreiras de permissão no nível da carga de trabalho](#)
- [Gire as chaves de acesso do IAM em um intervalo regular](#)
- [Identificar recursos que são compartilhados com uma entidade externa](#)

Monitore e configure notificações para a atividade do usuário root

Ao criar um pela primeira vez Conta da AWS, você começa com uma identidade de login único chamada usuário raiz. Por padrão, o usuário root tem acesso total a todos Serviços da AWS os recursos da conta. Você deve controlar e monitorar rigorosamente o usuário raiz e usá-lo somente para [tarefas que exijam credenciais de usuário raiz](#).

Para obter mais informações, consulte os seguintes recursos:

- [Conceda acesso com privilégios mínimos no Well-Architected Framework](#) AWS
- [Monitore a atividade do usuário raiz do IAM](#) na AWS orientação prescritiva

Não crie chaves de acesso para o usuário-raiz

O usuário raiz é o mais privilegiado em uma Conta da AWS. A desativação do acesso programático ao usuário raiz ajuda a reduzir o risco de exposição inadvertida das credenciais do usuário e o comprometimento subsequente do ambiente de nuvem. Recomendamos que você crie e use funções do IAM como credenciais temporárias para acessar seus recursos Contas da AWS e recursos.

Para obter mais informações, consulte os seguintes recursos:

- A [chave de acesso do usuário raiz do IAM não deve existir](#) na AWS Security Hub documentação
- [Excluindo chaves de acesso para o usuário raiz](#) na documentação do IAM
- [Funções do IAM](#) na documentação do IAM

Ativar o MFA para o usuário raiz

Recomendamos que você habilite vários dispositivos de autenticação multifator (MFA) para Conta da AWS o usuário raiz e os usuários do IAM. Isso aumenta a barreira de segurança Contas da AWS e pode simplificar o gerenciamento de acesso. Como um usuário root é um usuário altamente privilegiado que pode realizar ações privilegiadas, é crucial exigir MFA para o usuário root. Você pode usar um dispositivo de MFA de hardware que gera um código numérico com base no algoritmo de senha única baseada em tempo (TOTP), em uma chave de segurança de hardware FIDO ou em um aplicativo de autenticador virtual.

Em 2024, o MFA será necessário para acessar o usuário raiz de qualquer um. Conta da AWS Para obter mais informações, consulte [Secure by Design: AWS para aprimorar os requisitos de MFA em 2024 no AWS blog](#) de segurança. Recomendamos fortemente que você amplie essa prática de segurança e exija a MFA para todos os tipos de usuários em seus AWS ambientes.

Se possível, recomendamos que você use um dispositivo de MFA de hardware para o usuário root. A MFA virtual pode não fornecer o mesmo nível de segurança oferecido por dispositivos MFA de hardware. Você pode usar a MFA virtual enquanto aguarda a aprovação ou entrega da compra do hardware.

Em situações em que você gerencia centenas de contas AWS Organizations, dependendo da tolerância ao risco da sua organização, talvez não seja escalável usar a MFA baseada em hardware para o usuário raiz de cada conta em uma unidade organizacional (OU). Nesse caso, você pode

escolher uma conta na OU que atue como uma conta de gerenciamento da OU e, em seguida, desativar o usuário raiz para as outras contas nessa OU. Por padrão, a conta de gerenciamento da OU não tem acesso às outras contas. Ao configurar o acesso entre contas com antecedência, você pode acessar as outras contas da conta de gerenciamento da OU em caso de emergência. Para configurar o acesso entre contas, você cria uma função do IAM na conta do membro e define políticas para que somente o usuário raiz na conta de gerenciamento da OU possa assumir essa função. Para obter mais informações, consulte [Tutorial: Delegar acesso ao Contas da AWS uso de funções do IAM](#) na documentação do IAM.

Recomendamos que você habilite vários dispositivos de MFA para suas credenciais de usuário raiz. Você pode registrar até oito dispositivos de MFA de qualquer combinação.

Para obter mais informações, consulte os seguintes recursos:

- [Habilitando um token TOTP de hardware](#) na documentação do IAM
- [Habilitando um dispositivo virtual de autenticação multifator \(MFA\)](#) na documentação do IAM
- [Habilitando uma chave de segurança FIDO](#) na documentação do IAM
- [Proteja seu login de usuário raiz com a autenticação multifator \(MFA\) na](#) documentação do IAM

Siga as melhores práticas de segurança do IAM

A documentação do IAM inclui uma lista das melhores práticas projetadas para ajudar você a proteger seus Contas da AWS recursos. Ele inclui recomendações para configurar o acesso e as permissões de acordo com o princípio do privilégio mínimo. Exemplos das melhores práticas de segurança do IAM incluem a configuração da federação de identidades, a exigência de MFA e o uso de credenciais temporárias.

Para obter mais informações, consulte os seguintes recursos:

- [Melhores práticas de segurança no IAM](#) na documentação do IAM
- [Usando credenciais temporárias com AWS recursos](#) na documentação do IAM

Conceda permissões com privilégios mínimos

O privilégio mínimo é a prática de conceder somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser tomadas em recursos específicos sob condições específicas.

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos, como suas tags. Você pode usar atributos de grupo, identidade e recurso para definir dinamicamente as permissões em grande escala, em vez de definir permissões para usuários individuais. Por exemplo, você pode usar o ABAC para permitir que um grupo de desenvolvedores acesse somente recursos que tenham uma tag específica associada ao projeto.

Para obter mais informações, consulte os seguintes recursos:

- [Aplique permissões de privilégio mínimo](#) na documentação do IAM
- [Para que serve o ABAC AWS](#) na documentação do IAM

Defina barreiras de permissão no nível da carga de trabalho

É uma prática recomendada usar uma estratégia de várias contas, pois ela oferece flexibilidade para definir barreiras no nível da carga de trabalho. A Arquitetura de Referência de AWS Segurança oferece orientação prescritiva sobre como estruturar suas contas. Essas contas são gerenciadas como uma organização em [AWS Organizations](#), e as contas são agrupadas em unidades organizacionais (OUs).

Serviços da AWS, por exemplo [AWS Control Tower](#), podem ajudá-lo a gerenciar centralmente os controles em uma organização. Recomendamos que você defina uma finalidade clara para cada conta ou UO dentro da organização e aplique controles de acordo com essa finalidade. AWS Control Tower implementa controles preventivos, de detecção e proativos que ajudam você a controlar os recursos e monitorar a conformidade. Um controle preventivo é projetado para evitar que um evento ocorra. Um controle de detetive é projetado para detectar, registrar e alertar após a ocorrência de um evento. Um controle proativo foi projetado para impedir a implantação de recursos não compatíveis examinando os recursos antes de serem provisionados.

Para obter mais informações, consulte os seguintes recursos:

- [Cargas de trabalho separadas usando contas](#) no AWS Well-Architected Framework
- [AWS Arquitetura de referência de segurança \(AWS SRA\)](#) na orientação AWS prescritiva
- [Sobre os controles AWS Control Tower na](#) AWS Control Tower documentação
- [Implementando controles de segurança AWS](#) na AWS orientação prescritiva
- [Use políticas de controle de serviço para definir barreiras de permissão em todas as contas em sua AWS organização](#) no Blog de Segurança AWS

Gire as chaves de acesso do IAM em um intervalo regular

É uma prática recomendada atualizar as chaves de acesso para casos de uso que exigem credenciais de longo prazo. Recomendamos alternar as chaves de acesso a cada 90 dias ou menos. A rotação das chaves de acesso reduz o risco de que uma chave de acesso associada a uma conta comprometida ou encerrada seja usada. Também impede o acesso usando uma chave antiga que pode ter sido perdida, comprometida ou roubada. Sempre atualize os aplicativos depois de girar as teclas de acesso.

Para obter mais informações, consulte os seguintes recursos:

- [Atualize as chaves de acesso quando necessário para casos de uso que exigem credenciais de longo prazo](#) na documentação do IAM
- [Gire automaticamente as chaves de acesso do usuário do IAM em grande escala com AWS Organizations e AWS Secrets Manager](#) na orientação AWS prescritiva
- [Atualização das chaves de acesso](#) na documentação do IAM

Identificar recursos que são compartilhados com uma entidade externa

Uma entidade externa é um recurso, aplicativo, serviço ou usuário que está fora da sua AWS organização, como outro Contas da AWS usuário raiz, usuário ou função do IAM, usuário federado ou usuário anônimo (ou não autenticado). AWS service (Serviço da AWS) É uma prática recomendada de segurança usar o IAM Access Analyzer para identificar os recursos em sua organização e contas, como buckets do Amazon Simple Storage Service (Amazon S3) ou funções do IAM, que são compartilhados com uma entidade externa. Isso ajuda a identificar o acesso não intencional a recursos e dados, o que é um risco de segurança.

Para obter mais informações, consulte os seguintes recursos:

- [Verifique o acesso público e entre contas aos recursos com o IAM Access Analyzer na documentação](#) do IAM
- [Analise o acesso público e entre contas](#) no AWS Well-Architected Framework
- [Usando AWS Identity and Access Management Access Analyzer](#) na documentação do IAM

Recomendações de controle de segurança para registro e monitoramento

O registro e o monitoramento são aspectos importantes da detecção de ameaças. A detecção de ameaças é um dos recursos da perspectiva de segurança no [AWS Cloud Adoption Framework \(AWS CAF\)](#). Ao usar dados de log, sua organização pode monitorar seu ambiente para entender e identificar possíveis configurações incorretas de segurança, ameaças e comportamentos inesperados. Compreender as ameaças em potencial pode ajudar sua organização a priorizar os controles de segurança, e a detecção eficaz de ameaças pode ajudá-lo a responder às ameaças mais rapidamente.

Controles nesta seção:

- [Configure pelo menos uma trilha multirregional no CloudTrail](#)
- [Configurar o registro no nível do serviço e do aplicativo](#)
- [Estabeleça um local centralizado para analisar registros e responder a eventos de segurança](#)
- [Evite o acesso não autorizado aos buckets do S3 que contêm arquivos de log CloudTrail](#)
- [Configurar alertas para alterações nos grupos de segurança ou na rede ACLs](#)
- [Configurar alertas para CloudWatch alarmes que entram no estado ALARME](#)

Configure pelo menos uma trilha multirregional no CloudTrail

[AWS CloudTrail](#) ajuda você a auditar a governança, a conformidade e o risco operacional do seu Conta da AWS. As ações realizadas por um usuário, função ou um AWS service (Serviço da AWS) são registradas como eventos em CloudTrail. Os eventos incluem ações realizadas em AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs e APIs e. Esse histórico de eventos ajuda você a analisar sua postura de segurança, rastrear alterações de recursos e auditar a conformidade.

Para um registro contínuo dos eventos em seu Conta da AWS, você deve criar uma trilha. Cada trilha deve ser configurada para registrar todos os eventos Regiões da AWS. Ao registrar todos os eventos Regiões da AWS, você garante que todos os eventos que ocorrem no seu Conta da AWS sejam registrados, independentemente de onde Região da AWS tenham ocorrido. Uma trilha multirregional garante que os [eventos de serviços globais](#) sejam registrados.

Para obter mais informações, consulte os seguintes recursos:

- [CloudTrail melhores práticas de segurança de detetive](#) na documentação CloudTrail
- [Convertendo uma trilha que se aplica a uma região para se aplicar a todas as regiões](#) na documentação CloudTrail
- [Ativando e desativando o registro de eventos de serviços globais](#) na documentação CloudTrail

Configurar o registro no nível do serviço e do aplicativo

O AWS Well-Architected Framework recomenda que você retenha registros de eventos de segurança de serviços e aplicativos. Esse é um princípio fundamental de segurança para auditorias, investigações e casos de uso operacional. A retenção de registros de serviços e aplicativos é um requisito comum de segurança orientado por padrões, políticas e procedimentos de governança, risco e conformidade (GRC).

As equipes de operações de segurança confiam em registros e ferramentas de pesquisa para descobrir possíveis eventos de interesse que possam indicar atividades não autorizadas ou alterações não intencionais. Você pode ativar o registro em registros para diferentes serviços, dependendo do caso de uso. Por exemplo, você pode registrar o acesso ao bucket do Amazon S3, o tráfego AWS WAF da Web ACL, o tráfego do Amazon API Gateway na camada de rede ou as distribuições da Amazon. CloudFront

Para obter mais informações, consulte os seguintes recursos:

- [Transmita o Amazon CloudWatch Logs para uma conta centralizada para auditoria e análise](#) no Blog de AWS Arquitetura
- [Configure o registro de serviços e aplicativos](#) no AWS Well-Architected Framework

Estabeleça um local centralizado para analisar registros e responder a eventos de segurança

Analisar manualmente os registros e processar as informações é insuficiente para acompanhar o volume de informações associado a arquiteturas complexas. A análise e os relatórios por si só não facilitam a atribuição de eventos ao recurso correto em tempo hábil. O AWS Well-Architected Framework recomenda que você AWS integre eventos e descobertas de segurança em um sistema de notificação e fluxo de trabalho, como um sistema de emissão de tíquetes, bugs ou sistema de

gerenciamento de eventos e informações de segurança (SIEM). Esses sistemas ajudam você a atribuir, rotear e gerenciar eventos de segurança.

Para obter mais informações, consulte os seguintes recursos:

- [Analise registros, descobertas e métricas centralmente](#) no AWS Well-Architected Framework
- [Analise a segurança, a conformidade e a atividade operacional usando o CloudTrail Amazon Athena no AWS blog](#) de segurança
- [AWS Parceiros que fornecem serviços de detecção e resposta a ameaças](#) no portfólio de AWS parceiros

Evite o acesso não autorizado aos buckets do S3 que contêm arquivos de log CloudTrail

Por padrão, os arquivos de CloudTrail log são armazenados em buckets do Amazon S3. É uma prática recomendada de segurança impedir o acesso não autorizado a qualquer bucket do Amazon S3 que CloudTrail contenha arquivos de log. Isso ajuda você a manter a integridade, a integridade e a disponibilidade desses registros, o que é crucial para fins forenses e de auditoria. Se você quiser registrar eventos de dados para buckets do S3 que contêm arquivos de CloudTrail log, você pode criar uma CloudTrail trilha para essa finalidade.

Para obter mais informações, consulte os seguintes recursos:

- [Definindo configurações de bloqueio de acesso público para seus buckets do S3](#) na documentação do Amazon S3
- [CloudTrail melhores práticas de segurança preventiva na](#) documentação CloudTrail
- [Criando uma trilha](#) na CloudTrail documentação

Configurar alertas para alterações nos grupos de segurança ou na rede ACLs

Um grupo de segurança na Amazon Virtual Private Cloud (Amazon VPC) controla o tráfego que pode alcançar e sair dos recursos aos quais está associado. Uma lista de controle de acesso à rede (ACL) permite ou nega tráfego específico de entrada ou saída no nível da sub-rede da VPC. Esses recursos são essenciais para gerenciar o acesso em seu AWS ambiente.

Crie e configure um CloudWatch alarme da Amazon que notifique você se uma configuração de grupo de segurança ou ACL de rede for alterada. Configure esse alarme para alertá-lo sempre que uma chamada de AWS API for executada para atualizar grupos de segurança. Você também pode usar serviços, como [Amazon EventBridge](#) e [AWS Config](#), para responder automaticamente a esses tipos de eventos de segurança.

Para obter mais informações, consulte os seguintes recursos:

- [Reverta e receba automaticamente notificações sobre alterações em seus grupos de segurança da Amazon VPC no AWS Security Blog](#)
- [Usando CloudWatch alarmes da Amazon](#) na documentação CloudWatch
- [Implemente eventos de segurança acionáveis](#) no AWS Well-Architected Framework
- [Automatize a resposta a eventos](#) no AWS Well-Architected Framework

Configurar alertas para CloudWatch alarmes que entram no estado ALARME

Em CloudWatch, você pode especificar quais ações um alarme executa quando muda de estado entre os INSUFFICIENT_DATA estados OKALARM, e. O tipo mais comum de ação de alarme é notificar uma ou mais pessoas enviando uma mensagem para um tópico do Amazon Simple Notification Service (Amazon SNS). Você também pode configurar alarmes para criar [OpsItems](#) ou [incidentes](#) em. AWS Systems Manager

Recomendamos que você ative as ações de alarme para alertar automaticamente se uma métrica monitorada estiver fora do limite definido. O monitoramento de alarmes ajuda você a identificar atividades incomuns e a responder rapidamente a problemas operacionais e de segurança.

Para obter mais informações, consulte os seguintes recursos:

- [Implemente eventos de segurança acionáveis](#) no AWS Well-Architected Framework
- [Ações de alarme](#) na CloudWatch documentação

Recomendações de controle de segurança para proteger a infraestrutura

A proteção da infraestrutura é uma parte fundamental de qualquer programa de segurança. Ele inclui metodologias de controle que ajudam você a proteger suas redes e recursos computacionais. Exemplos de proteção de infraestrutura incluem limites de confiança, uma defense-in-depth abordagem, fortalecimento da segurança, gerenciamento de patches e autenticação e autorização do sistema operacional. Para obter mais informações, consulte [Proteção de infraestrutura](#) no AWS Well-Architected Framework. Os controles de segurança nesta seção podem ajudá-lo a implementar as melhores práticas para proteção da infraestrutura.

Controles nesta seção:

- [Especifique objetos raiz padrão para CloudFront distribuições](#)
- [Digitalize o código do aplicativo para identificar problemas comuns de segurança](#)
- [Crie camadas de rede usando redes dedicadas VPCs e sub-redes](#)
- [Restrinja o tráfego de entrada somente às portas autorizadas](#)
- [Bloquear o acesso público aos documentos do Systems Manager](#)
- [Bloqueie o acesso público às funções do Lambda](#)
- [Restrinja o tráfego de entrada e saída no grupo de segurança padrão](#)
- [Verifique se há vulnerabilidades de software e exposição não intencional na rede](#)
- [Configurar AWS WAF](#)
- [Configure proteções avançadas contra ataques DDoS](#)
- [Use uma defense-in-depth abordagem para controlar o tráfego de rede](#)

Especifique objetos raiz padrão para CloudFront distribuições

[A Amazon CloudFront](#) acelera a distribuição do seu conteúdo da web entregando-o por meio de uma rede mundial de data centers, o que reduz a latência e melhora o desempenho. Se você não definir um objeto raiz padrão, as solicitações da raiz da distribuição passarão para o servidor de origem. Se você estiver usando uma origem do Amazon Simple Storage Service (Amazon S3), a solicitação pode retornar uma lista do conteúdo em seu bucket do S3 ou uma lista do conteúdo privado de sua origem. Especificar um objeto raiz padrão ajuda a evitar a exposição do conteúdo da sua distribuição.

Para obter mais informações, consulte os seguintes recursos:

- [Especificando um objeto raiz padrão](#) na documentação CloudFront

Digitalize o código do aplicativo para identificar problemas comuns de segurança

O AWS Well-Architected Framework recomenda que você escaneie bibliotecas e dependências em busca de problemas e defeitos. Há muitas ferramentas de análise de código-fonte que você pode usar para escanear o código-fonte. Por exemplo, a Amazon CodeGuru pode verificar problemas de segurança comuns no Java or Python aplicativos e forneça recomendações para remediação.

Para obter mais informações, consulte os seguintes recursos:

- [CodeGuru documentação](#)
- [Ferramentas de análise de código-fonte](#) no OWASP Foundation site
- [Execute o gerenciamento de vulnerabilidades](#) no AWS Well-Architected Framework

Crie camadas de rede usando redes dedicadas VPCs e sub-redes

O AWS Well-Architected Framework recomenda que você agrupe componentes que compartilham requisitos de sensibilidade em camadas. Isso minimiza o escopo potencial do impacto do acesso não autorizado. Por exemplo, um cluster de banco de dados que não exige acesso à Internet deve ser colocado em uma sub-rede privada de sua VPC para garantir que não haja nenhuma rota de ou para a Internet.

AWS oferece muitos serviços que podem ajudá-lo a testar e identificar a acessibilidade pública. Por exemplo, o Reachability Analyzer é uma ferramenta de análise de configuração que ajuda você a testar a conectividade entre os recursos de origem e destino em seu VPCs. Além disso, o Network Access Analyzer pode ajudá-lo a identificar o acesso não intencional à rede aos recursos.

Para obter mais informações, consulte os seguintes recursos:

- [Crie camadas de rede](#) no AWS Well-Architected Framework
- [Documentação do Reachability Analyzer](#)
- [Documentação do Network Access Analyzer](#)

- [Crie uma sub-rede](#) na documentação da Amazon Virtual Private Cloud (Amazon VPC)

Restrinja o tráfego de entrada somente às portas autorizadas

O acesso irrestrito, como o tráfego do endereço IP de $0.0.0.0/0$ origem, aumenta o risco de atividades maliciosas, como invasões, ataques (denial-of-serviceDoS) e perda de dados. Os grupos de segurança fornecem filtragem com estado do tráfego de entrada e saída da rede para os recursos. AWS Nenhum grupo de segurança deve permitir acesso irrestrito a portas conhecidas, como SSH e Windows protocolo de desktop remoto (RDP). Para tráfego de entrada, em seus grupos de segurança, permita somente conexões TCP ou UDP em portas autorizadas. Para se conectar às instâncias do Amazon Elastic Compute Cloud (Amazon EC2), use o [Session Manager](#) ou o [Run Command](#) em vez do acesso direto por SSH ou RDP.

Para obter mais informações, consulte os seguintes recursos:

- [Trabalhe com grupos de segurança](#) na EC2 documentação da Amazon
- [Controle o tráfego para seus AWS recursos usando grupos de segurança](#) na documentação da Amazon VPC

Bloquear o acesso público aos documentos do Systems Manager

A menos que seu caso de uso exija que o compartilhamento público seja ativado, as AWS Systems Manager melhores práticas recomendam que você bloqueie o compartilhamento público de documentos do Systems Manager. O compartilhamento público pode fornecer acesso não intencional aos documentos. Um documento público do Systems Manager pode expor informações valiosas e confidenciais sobre sua conta, recursos e processos internos.

Para obter mais informações, consulte os seguintes recursos:

- [Melhores práticas para documentos compartilhados do Systems Manager](#) na documentação do Systems Manager
- [Modificar permissões para um documento compartilhado do Systems Manager](#) na documentação do Systems Manager

Bloqueie o acesso público às funções do Lambda

O [AWS Lambda](#) é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. As funções Lambda não devem ser acessíveis ao público, pois isso pode permitir acesso não intencional ao código da função.

Recomendamos que você configure [políticas baseadas em recursos para funções do Lambda](#) para negar acesso de fora da sua conta. Você pode fazer isso removendo as permissões ou adicionando a `AWS:SourceAccount` condição à declaração que permite o acesso. Você pode atualizar políticas baseadas em recursos para funções do Lambda por meio da API Lambda ou (). AWS Command Line Interface AWS CLI

Também recomendamos que você habilite a função [Lambda.1]. As políticas da função Lambda devem proibir o controle de acesso público em. AWS Security Hub Esse controle valida que as políticas baseadas em recursos para funções do Lambda proíbem o acesso público.

Para obter mais informações, consulte os seguintes recursos:

- [AWS Lambda controles](#) na documentação do Security Hub
- [Usando políticas baseadas em recursos para o Lambda na documentação do Lambda](#)
- [Recursos e condições para ações do Lambda](#) na documentação do Lambda

Restrinja o tráfego de entrada e saída no grupo de segurança padrão

Se você não associar um grupo de segurança personalizado ao provisionar um AWS recurso, o recurso será associado ao grupo de segurança padrão da VPC. As regras padrão para esse grupo de segurança permitem todo o tráfego de entrada de todos os recursos atribuídos a esse grupo de segurança e permitem todo o tráfego de saída IPv4 e IPv6 de saída. Isso pode permitir tráfego não intencional para o recurso.

AWS recomenda que você não use o grupo de segurança padrão. Em vez disso, crie grupos de segurança personalizados para recursos específicos ou grupos de recursos.

Como o grupo de segurança padrão não pode ser excluído, recomendamos que você altere as regras do grupo de segurança padrão para restringir o tráfego de entrada e saída. Ao configurar as regras do grupo de segurança, siga o princípio do [menor privilégio](#).

Também recomendamos que você ative o [EC2.2] Os grupos de segurança padrão da VPC não devem permitir o controle de tráfego de entrada ou saída no Security Hub. Esse controle valida que o grupo de segurança padrão de uma VPC nega tráfego de entrada e saída.

Para obter mais informações, consulte os seguintes recursos:

- [Controle o tráfego para seus AWS recursos usando grupos de segurança na documentação da Amazon VPC](#)
- [Grupos de segurança padrão para você VPCs](#) na documentação da Amazon VPC
- [EC2Controles da Amazon](#) na documentação do Security Hub

Verifique se há vulnerabilidades de software e exposição não intencional na rede

Recomendamos que você habilite o Amazon Inspector em todas as suas contas. [O Amazon Inspector](#) é um serviço de gerenciamento de vulnerabilidades que verifica continuamente suas EC2 instâncias da Amazon, imagens de contêineres do Amazon Elastic Container Registry (Amazon ECR) e funções Lambda em busca de vulnerabilidades de software e exposição não intencional na rede. Ele também oferece suporte à inspeção profunda das EC2 instâncias da Amazon. Quando o Amazon Inspector identifica uma vulnerabilidade ou um caminho de rede aberto, ele produz uma descoberta que você pode investigar. Se o Amazon Inspector e o Security Hub estiverem configurados em sua conta, o Amazon Inspector enviará automaticamente as descobertas de segurança ao Security Hub para gerenciamento centralizado.

Para obter mais informações, consulte os seguintes recursos:

- [Digitalizando recursos com o Amazon Inspector na documentação](#) do Amazon Inspector
- [Inspeção profunda do Amazon Inspector para a Amazon EC2 na documentação do Amazon Inspector](#)
- [Digitalize EC2 AMIs usando o Amazon Inspector](#) no Blog de Segurança AWS
- [Construindo um programa escalável de gerenciamento de vulnerabilidades AWS na Orientação AWS Prescritiva](#)
- [Automatize a proteção de rede](#) no AWS Well-Architected Framework
- [Automatize a proteção computacional no AWS Well-Architected Framework](#)

Configurar AWS WAF

[AWS WAF](#) é um firewall de aplicativo web que ajuda você a monitorar e bloquear solicitações HTTP ou HTTPS que são encaminhadas para seus recursos protegidos de aplicativos web, como Amazon API Gateway APIs, CloudFront distribuições da Amazon ou Application Load Balancers. Com base nos critérios que você especifica, o serviço responde às solicitações com o conteúdo solicitado, com um código de status HTTP 403 (Proibido) ou com uma resposta personalizada. AWS WAF pode ajudar a proteger aplicativos da Web ou APIs contra explorações comuns da Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos. Considere configurar AWS WAF Contas da AWS e usar uma combinação de regras AWS gerenciadas, regras personalizadas e integrações de parceiros para ajudar a proteger seus aplicativos contra ataques na camada de aplicativos (camada 7).

Para obter mais informações, consulte os seguintes recursos:

- [Introdução AWS WAF](#) na AWS WAF documentação
- [AWS WAF parceiros de entrega](#) no AWS site
- [Automações de segurança para AWS WAF](#) a Biblioteca de AWS Soluções
- [Implemente inspeção e proteção](#) no AWS Well-Architected Framework

Configure proteções avançadas contra ataques DDo S

[AWS Shield](#) fornece proteções contra ataques distribuídos de negação de serviço (DDoS) para AWS recursos nas camadas de rede e transporte (camadas 3 e 4) e na camada de aplicação (camada 7). Este serviço está disponível em duas opções: AWS Shield Standard e AWS Shield Advanced. O Shield Standard protege automaticamente AWS os recursos suportados, sem custo adicional.

Recomendamos que você assine o Shield Advanced, que fornece proteção expandida contra ataques DDo S para recursos protegidos. As proteções que você recebe do Shield Advanced variam de acordo com suas opções de arquitetura e configuração. Considere a implementação das proteções do Shield Advanced para aplicativos em que você precisa de qualquer um dos seguintes:

- Disponibilidade garantida para os usuários do aplicativo.
- Acesso rápido a especialistas em mitigação de DDo S se o aplicativo for afetado por um ataque DDo S.

- Conscientização da AWS de que o aplicativo pode ser afetado por um ataque DDo S e notificação de ataques da AWS e escalonamento para suas equipes de segurança ou operações.
- Previsibilidade em seus custos de nuvem, inclusive quando um ataque DDo S afeta seu uso de Serviços da AWS

Para obter mais informações, consulte os seguintes recursos:

- [AWS Shield Advanced visão geral](#) na documentação do Shield
- [AWS Shield Advanced recursos protegidos](#) na documentação do Shield
- [AWS Shield Advanced capacidades e opções](#) na documentação do Shield
- [Respondendo aos eventos DDo S](#) na documentação do Shield
- [Implemente inspeção e proteção](#) no AWS Well-Architected Framework

Use uma defense-in-depth abordagem para controlar o tráfego de rede

AWS Network Firewall é um serviço gerenciado e estável de firewall de rede e detecção e prevenção de intrusões para nuvens privadas virtuais (VPCs) no. Nuvem AWS Ele ajuda você a implantar proteções de rede essenciais no perímetro da VPC. Isso inclui filtrar o tráfego que entra e vem de um gateway de Internet, gateway NAT ou por VPN ou. AWS Direct Connect O Firewall de Rede inclui recursos que ajudam a proteger contra ameaças comuns à rede. O firewall com estado no Firewall de Rede pode incorporar o contexto dos fluxos de tráfego, como conexões e protocolos, para aplicar políticas.

Para obter mais informações, consulte os seguintes recursos:

- [AWS Network Firewall documentação](#)
- [Controle o tráfego em todas as camadas no](#) AWS Well-Architected Framework

Recomendações de controle de segurança para proteger dados

O AWS Well-Architected Framework agrupa as melhores práticas para proteção de dados em três categorias: classificação de dados, proteção de dados em repouso e proteção de dados em trânsito. Os controles de segurança nesta seção podem ajudá-lo a implementar as melhores práticas de proteção de dados. Essas melhores práticas básicas devem estar em vigor antes de você arquitetar qualquer carga de trabalho na nuvem. Eles evitam o manuseio incorreto de dados e ajudam você a cumprir as obrigações organizacionais, regulatórias e de conformidade. Use os controles de segurança nesta seção para implementar as melhores práticas de proteção de dados.

Controles nesta seção:

- [Identifique e classifique os dados no nível da carga de trabalho](#)
- [Estabeleça controles para cada nível de classificação de dados](#)
- [Criptografe dados em repouso](#)
- [Criptografe dados em trânsito](#)
- [Bloqueie o acesso público aos snapshots do Amazon EBS](#)
- [Bloqueie o acesso público aos snapshots do Amazon RDS](#)
- [Bloqueie o acesso público ao Amazon RDS, Amazon Redshift e recursos AWS DMS](#)
- [Bloqueie o acesso público aos buckets do Amazon S3](#)
- [Exigir MFA para excluir dados em buckets críticos do Amazon S3](#)
- [Configurar domínios OpenSearch do Amazon Service em uma VPC](#)
- [Configurar alertas para AWS KMS key exclusão](#)
- [Bloquear o acesso público ao AWS KMS keys](#)
- [Configurar ouvintes do balanceador de carga para usar protocolos seguros](#)

Identifique e classifique os dados no nível da carga de trabalho

Classificação de dados é 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 geralmente reduz a frequência da duplicação de dados. Isso pode reduzir os custos de armazenamento e backup e acelerar as pesquisas.

Recomendamos que você entenda o tipo e a classificação dos dados que sua carga de trabalho está processando, os processos comerciais associados, onde os dados são armazenados e quem é o proprietário dos dados. A classificação de dados ajuda os proprietários da carga de trabalho a identificar locais que armazenam dados confidenciais e determinar como esses dados devem ser acessados e compartilhados. As tags são pares de valores-chave que atuam como metadados para organizar os recursos. AWS As tags podem ajudar a gerenciar, identificar, organizar, pesquisar e filtrar recursos.

Para obter mais informações, consulte os seguintes recursos:

- [Classificação de dados](#) em AWS whitepapers
- [Identifique os dados em sua carga de trabalho no](#) AWS Well-Architected Framework

Estabeleça controles para cada nível de classificação de dados

Defina controles de proteção de dados para cada nível de classificação. Por exemplo, use controles recomendados para proteger dados classificados como públicos e proteger dados confidenciais com controles adicionais. Use mecanismos e ferramentas que reduzam ou eliminem a necessidade de acessar diretamente ou processar dados manualmente. A automação da identificação e classificação de dados reduz o risco de erros de classificação, manuseio incorreto, modificação ou erro humano.

Por exemplo, considere usar o Amazon Macie para escanear buckets do Amazon Simple Storage Service (Amazon S3) em busca de dados confidenciais, como informações de identificação pessoal (PII). Além disso, você pode automatizar a detecção de acesso não intencional a dados usando VPC Flow Logs na Amazon Virtual Private Cloud (Amazon VPC).

Para obter mais informações, consulte os seguintes recursos:

- [Defina os controles de proteção de dados](#) no AWS Well-Architected Framework
- [Automatize a identificação e a classificação](#) no AWS Well-Architected Framework
- [AWS Arquitetura de referência de privacidade \(AWS PRA\)](#) na AWS orientação prescritiva
- [Descobrimo dados confidenciais com o Amazon Macie](#) na documentação do Macie
- [Registrando tráfego IP usando VPC Flow Logs na documentação](#) da Amazon VPC

- [Técnicas comuns para detectar dados de PHI e PII usando Serviços da AWS](#) no blog AWS for Industries

Criptografe dados em repouso

Dados em repouso são dados estacionários em sua rede, como dados que estão armazenados. A implementação de criptografia e controles de acesso apropriados para dados em repouso ajuda a reduzir o risco de acesso não autorizado. A criptografia é um processo de computação que transforma dados de texto simples, legíveis por humanos, em texto cifrado. Você precisa de uma chave de criptografia para descriptografar o conteúdo novamente em texto simples para que ele possa ser usado. No Nuvem AWS, você pode usar AWS Key Management Service (AWS KMS) para criar e controlar chaves criptográficas que ajudam a proteger seus dados.

Conforme discutido em [Estabeleça controles para cada nível de classificação de dados](#), recomendamos a criação de uma política que especifique que tipo de dados requer criptografia. Inclua critérios para determinar quais dados devem ser criptografados e quais dados devem ser protegidos com outra técnica, como tokenização ou hashing.

Para obter mais informações, consulte os seguintes recursos:

- [Configurando a criptografia padrão](#) na documentação do Amazon S3
- [Criptografia por padrão para novos volumes do EBS e cópias de snapshot](#) na documentação da Amazon EC2
- [Criptografando recursos do Amazon Aurora](#) na documentação do Amazon Aurora
- [Introdução aos detalhes criptográficos AWS KMS da](#) documentação AWS KMS
- [Criação de uma estratégia de criptografia corporativa para dados em repouso na Orientação AWS Prescritiva](#)
- [Aplique a criptografia em repouso no](#) AWS Well-Architected Framework
- Para obter mais informações sobre criptografia em particular Serviços da AWS, consulte a [AWS documentação](#) desse serviço

Criptografe dados em trânsito

Dados em trânsito que estão se movendo ativamente pela sua rede, como entre os recursos da rede. Criptografe todos os dados em trânsito usando protocolos TLS seguros e pacotes de criptografia. O

tráfego de rede entre os recursos e a Internet deve ser criptografado para ajudar a impedir o acesso não autorizado aos dados. Quando possível, use o TLS para criptografar o tráfego de rede em seu ambiente interno AWS .

Para obter mais informações, consulte os seguintes recursos:

- [Exigir HTTPS para comunicação entre espectadores e CloudFront](#) na CloudFront documentação da Amazon
- [Documentação da AWS PrivateLink](#)
- [Aplique a criptografia em trânsito no](#) AWS Well-Architected Framework
- Para obter mais informações sobre criptografia em particular Serviços da AWS, consulte a [AWS documentação](#) desse serviço

Bloqueie o acesso público aos snapshots do Amazon EBS

[O Amazon Elastic Block Store \(Amazon EBS\)](#) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon Elastic Compute Cloud (Amazon). EC2 Você pode fazer backup dos dados dos seus volumes do Amazon EBS no Amazon S3 tirando point-in-time snapshots. Você pode compartilhar instantâneos publicamente com todos os outros Contas da AWS ou compartilhá-los de forma privada com a pessoa Contas da AWS que você especificar.

Recomendamos que você não compartilhe publicamente os snapshots do Amazon EBS. Isso pode inadvertidamente expor dados confidenciais. Ao compartilhar um instantâneo, você está dando a outras pessoas acesso aos dados no instantâneo. Compartilhe instantâneos somente com pessoas em quem você confia todos esses dados.

Para obter mais informações, consulte os seguintes recursos:

- [Compartilhe um instantâneo](#) na documentação da Amazon EC2
- [Os snapshots do Amazon EBS não devem ser restauráveis publicamente](#) na documentação AWS Security Hub
- [ebs-snapshot-public-restorable-verifique](#) a documentação AWS Config

Bloqueie o acesso público aos snapshots do Amazon RDS

O [Amazon Relational Database Service \(Amazon RDS\)](#) ajuda você a configurar, operar e escalar um banco de dados relacional no. Nuvem AWS O Amazon RDS cria e salva backups automatizados de sua instância de banco de dados (DB) ou cluster de banco de dados Multi-AZ durante a janela de backup de sua instância de banco de dados. O Amazon RDS cria um snapshot do volume de armazenamento de sua instância de banco de dados, fazendo o backup de toda a instância de banco de dados, não apenas dos bancos de dados individuais. Você pode compartilhar um snapshot manual com o objetivo de copiar o snapshot ou restaurar uma instância de banco de dados a partir dele.

Se você compartilhar um instantâneo como público, certifique-se de que nenhum dos dados no instantâneo seja privado ou confidencial. Quando um instantâneo é compartilhado publicamente, ele dá todas as Contas da AWS permissões para acessar os dados. Isso pode resultar na exposição não intencional dos dados em sua instância do Amazon RDS.

Para obter mais informações, consulte os seguintes recursos:

- [Compartilhamento de um DB snapshot](#) na documentação do Amazon RDS
- [rds-snapshots-public-prohibited](#) na AWS Config documentação
- O [instantâneo do RDS deve ser privado na documentação](#) do Security Hub

Bloqueie o acesso público ao Amazon RDS, Amazon Redshift e recursos AWS DMS

Você pode configurar instâncias de banco de dados do Amazon RDS, clusters do Amazon Redshift AWS Database Migration Service e AWS DMS() instâncias de replicação para serem acessíveis publicamente. Se o valor do `publiclyAccessible` campo for `true`, esses recursos estarão acessíveis ao público. Permitir o acesso público pode resultar em tráfego, exposição ou vazamentos de dados desnecessários. Recomendamos que você não permita o acesso público a esses recursos.

Recomendamos que você habilite AWS Config regras ou controles do Security Hub para detectar se as instâncias de banco de dados do Amazon RDS, as instâncias de AWS DMS replicação ou os clusters do Amazon Redshift permitem acesso público.

Note

As configurações de acesso público para instâncias AWS DMS de replicação não podem ser modificadas após o provisionamento da instância. Para alterar a configuração de acesso público, exclua a instância atual e, em seguida, recrie-a. Ao recriá-la, não selecione a opção Acessível publicamente.

Para obter mais informações, consulte os seguintes recursos:

- [AWS DMS instâncias de replicação não devem ser públicas](#) na documentação do Security Hub
- As [instâncias de banco de dados do RDS devem proibir o acesso público na documentação](#) do Security Hub
- [Os clusters do Amazon Redshift devem proibir o acesso público](#) na documentação do Security Hub
- [rds-instance-public-access-verifique](#) a documentação AWS Config
- [dms-replication-not-public](#) na AWS Config documentação
- [redshift-cluster-public-access-verifique](#) a documentação AWS Config
- [Modificando uma instância de banco de dados do Amazon RDS](#) na documentação do Amazon RDS
- [Modificação de um cluster](#) na documentação do Amazon Redshift

Bloqueie o acesso público aos buckets do Amazon S3

É uma prática recomendada de segurança do Amazon S3 para garantir que seus buckets não sejam acessíveis ao público. A menos que você exija explicitamente que qualquer pessoa na Internet possa ler ou gravar em seu bucket, certifique-se de que seu bucket não seja público. Isso ajuda a proteger a integridade e a segurança dos dados. Você pode usar AWS Config regras e controles do Security Hub para confirmar se seus buckets do Amazon S3 estão em conformidade com essa melhor prática.

Para obter mais informações, consulte os seguintes recursos:

- [Melhores práticas de segurança do Amazon S3 na documentação](#) do Amazon S3
- A [configuração do S3 Block Public Access deve ser habilitada](#) na documentação do Security Hub
- Os [buckets do S3 devem proibir o acesso público de leitura](#) na documentação do Security Hub

- Os [buckets do S3 devem proibir o acesso público de gravação](#) na documentação do Security Hub
- [bucket-public-read-prohibited regra s3-](#) na documentação AWS Config
- [s3- bucket-public-write-prohibited](#) na documentação AWS Config

Exigir MFA para excluir dados em buckets críticos do Amazon S3

Ao trabalhar com o Versionamento do S3 em buckets do Amazon S3, você pode, opcionalmente, adicionar outra camada de segurança configurando um bucket para habilitar a [exclusão de MFA \(autenticação multifator\)](#). Quando você faz isso, o proprietário do bucket precisa incluir dois formulários de autenticação em qualquer solicitação para excluir uma versão ou modificar o estado de versionamento do bucket. Recomendamos que você habilite esse recurso para buckets que contêm dados essenciais para sua organização. Isso pode evitar exclusões acidentais de buckets e dados.

Para obter mais informações, consulte os seguintes recursos:

- [Configurando a exclusão de MFA](#) na documentação do Amazon S3

Configurar domínios OpenSearch do Amazon Service em uma VPC

O Amazon OpenSearch Service é um serviço gerenciado que ajuda você a implantar, operar e escalar OpenSearch clusters no Nuvem AWS. O Amazon OpenSearch Service oferece suporte OpenSearch e legado Elasticsearch software de código aberto (OSS). Os domínios do Amazon OpenSearch Service implantados em uma VPC podem se comunicar com recursos da VPC pela AWS rede privada, sem a necessidade de atravessar a Internet pública. Essa configuração melhora sua postura de segurança ao restringir o acesso aos dados em trânsito. Recomendamos que você não anexe domínios do Amazon OpenSearch Service a sub-redes públicas e que a VPC seja configurada de acordo com as melhores práticas.

Para obter mais informações, consulte os seguintes recursos:

- [Lançamento de seus domínios do Amazon OpenSearch Service em uma VPC](#) na documentação do Amazon OpenSearch Service
- [opensearch-in-vpc-only](#) na AWS Config documentação

- [OpenSearch os domínios devem estar em uma VPC](#) na documentação do Security Hub

Configurar alertas para AWS KMS key exclusão

AWS Key Management Service (AWS KMS) as chaves não podem ser recuperadas depois de serem excluídas. Se uma chave KMS for excluída, os dados que ainda estiverem criptografados sob essa chave ficarão permanentemente irrecuperáveis. Se precisar manter o acesso aos dados, antes de excluir a chave, você deverá descriptografar os dados ou recriptografá-los com uma nova chave KMS. Só exclua uma chave do KMS quando você tiver certeza de que não vai mais precisar dela.

Recomendamos que você configure um CloudWatch alarme da Amazon que o notifique se alguém iniciar a exclusão de uma chave KMS. Como é destrutivo e potencialmente perigoso excluir uma chave KMS, é AWS KMS necessário definir um período de espera e programar a exclusão em 7 a 30 dias. Isso oferece a oportunidade de revisar a exclusão programada e cancelá-la, se necessário.

Para obter mais informações, consulte os seguintes recursos:

- [Agendamento e cancelamento da exclusão da chave](#) na documentação AWS KMS
- [Criação de um alarme que detecta o uso de uma chave KMS com exclusão pendente](#) na documentação AWS KMS
- [AWS KMS keys não deve ser excluído acidentalmente na documentação](#) do Security Hub

Bloquear o acesso público ao AWS KMS keys

As [principais políticas](#) são a principal forma de controlar o acesso AWS KMS keys a. Cada chave do KMS tem exatamente uma política de chaves. Permitir acesso anônimo às chaves do KMS pode levar a um vazamento de dados confidenciais. Recomendamos que você identifique todas as chaves KMS acessíveis ao público e atualize suas políticas de acesso para evitar solicitações não assinadas feitas a esses recursos.

Para obter mais informações, consulte os seguintes recursos:

- [As melhores práticas de segurança AWS Key Management Service](#) estão na AWS KMS documentação
- [Alterando uma política importante](#) na AWS KMS documentação
- [Determinando o AWS KMS keys acesso](#) à AWS KMS documentação

Configurar ouvintes do balanceador de carga para usar protocolos seguros

O [Elastic Load Balancing](#) distribui automaticamente o tráfego de entrada do aplicativo em vários destinos. Você configura seu load balancer para aceitar o tráfego de entrada especificando um ou mais listeners. Um receptor é um processo que verifica solicitações de conexão usando o protocolo e a porta configurados por você. Cada tipo de balanceador de carga oferece suporte a diferentes protocolos e portas:

- Os [Application Load Balancers](#) tomam decisões de roteamento na camada do aplicativo e usam protocolos HTTP ou HTTPS.
- Os [balanceadores de carga de rede](#) tomam decisões de roteamento na camada de transporte e usam os protocolos TCP, TLS, UDP ou TCP_UDP.
- Os [balanceadores de carga clássicos](#) tomam decisões de roteamento na camada de transporte (usando protocolos TCP ou SSL) ou na camada de aplicação (usando protocolos HTTP ou HTTPS).

Recomendamos que você sempre use protocolos HTTPS ou TLS. Esses protocolos garantem que o balanceador de carga seja responsável por criptografar e descriptografar o tráfego entre o cliente e o destino.

Para obter mais informações, consulte os seguintes recursos:

- [Ouvintes de seus Application Load Balancers na documentação](#) do Elastic Load Balancing
- [Ouvintes do seu Classic Load Balancer](#) na documentação do Elastic Load Balancing
- [Ouvintes de seus Network Load Balancers](#) na documentação do Elastic Load Balancing
- [Garanta que os balanceadores de AWS carga usem protocolos de escuta seguros na AWS Orientação Prescritiva](#)
- [elb-tls-https-listeners-somente](#) na documentação AWS Config
- [Os ouvintes do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS na documentação do Security Hub](#)
- [O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS na documentação do Security Hub](#)

Recomendações de segurança para responder a incidentes

Quando ocorre um evento de segurança em sua organização, seus usuários devem estar preparados para responder ao problema. Todos os usuários devem ter uma compreensão básica dos processos de resposta de segurança da sua organização. Planejamento, treinamento e experiência são essenciais para um programa bem-sucedido de resposta a incidentes. Idealmente, você prepara sua organização antes que ocorra um possível evento de segurança. O AWS Well-Architected Framework identifica três fundamentos necessários para um programa bem-sucedido de resposta a incidentes na nuvem: preparação, operações e atividade pós-incidente. Para obter mais informações, consulte [Aspectos da resposta a AWS incidentes](#) no AWS Well-Architected Framework.

Com exceção dos controles de segurança que notificam você sobre eventos ou respondem automaticamente a eles, há controles limitados que você pode estabelecer para a resposta a incidentes. Uma postura forte de resposta a incidentes é estabelecida principalmente por meio dos planos, processos, manuais, manuais e programas de treinamento que você usa em sua organização. Você pode usar os controles e recomendações desta seção para implementar as melhores práticas para seu programa de resposta a incidentes. Para obter mais informações sobre as melhores práticas para resposta a incidentes e orientação de implementação, consulte [Resposta a incidentes no AWS Well-Architected Framework](#).

Recomendações nesta seção:

- [Defina um plano de resposta a incidentes](#)
- [Crie e mantenha runbooks e manuais de resposta a incidentes](#)
- [Implemente automação de segurança orientada por eventos](#)
- [Documente como as equipes operacionais devem interagir com Suporte](#)
- [Configurar alertas para eventos de segurança](#)

Defina um plano de resposta a incidentes

Estabeleça um plano de resposta a incidentes (IRP) bem definido. O plano de resposta a incidentes foi projetado para ser a base do seu programa de resposta a incidentes. Esse plano deve ser personalizado para atender às necessidades de cada organização.

Para obter mais informações, consulte os seguintes recursos:

- [Desenvolva e teste um plano de resposta a incidentes](#) no Guia de resposta a incidentes de AWS segurança
- [Desenvolva planos de gerenciamento de incidentes](#) no AWS Well-Architected Framework
- [Identifique o pessoal chave e os recursos externos](#) no AWS Well-Architected Framework

Crie e mantenha runbooks e manuais de resposta a incidentes

Uma parte fundamental da preparação para um processo de resposta a incidentes é o desenvolvimento de manuais. Os manuais de resposta a incidentes fornecem uma série de etapas recomendadas que os usuários seguem quando ocorre um evento de segurança. Ter uma estrutura e etapas claras simplifica a resposta e reduz a probabilidade de erro humano.

Para obter mais informações, consulte os seguintes recursos:

- [Para que criar manuais](#) no Guia de Resposta a Incidentes AWS de Segurança
- [AWS exemplos de manuais de resposta a incidentes](#) em GitHub
- [Desenvolva e teste manuais de resposta a incidentes de segurança](#) no AWS Well-Architected Framework

Implemente automação de segurança orientada por eventos

A automação da resposta de segurança é 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 EC2 da Amazon ou a rotação de credenciais.

Muitos Serviços da AWS oferecem suporte a respostas automatizadas. Por exemplo, você pode configurar um CloudWatch alarme da Amazon para métricas específicas, e o alarme pode iniciar uma ação quando o alarme muda de estado. Através da Amazon EventBridge, você também pode configurar respostas e remediações automáticas para descobertas no Amazon AWS Security Hub Inspector.

Para obter mais informações, consulte os recursos abaixo:

- [Corrija automaticamente as descobertas de segurança do Amazon Inspector no AWS Blog de Segurança](#)
- [Comece a usar a automação de respostas de AWS segurança AWS no Blog de Segurança](#)
- [Resposta de segurança automatizada AWS](#) ativada na Biblioteca de AWS Soluções
- [Usando CloudWatch alarmes da Amazon](#) na documentação CloudWatch
- [Resposta e remediação automatizadas](#) na documentação do Security Hub
- [Criação de respostas personalizadas às descobertas do Amazon Inspector com a Amazon EventBridge na documentação do Amazon Inspector](#)

Documente como as equipes operacionais devem interagir com Suporte

Para você Conta da AWS, você pode definir um contato principal e três contatos alternativos. Recomendamos que você forneça um contato de segurança para cada um Conta da AWS ou para sua organização.

AWS Support oferece uma variedade de planos que fornecem acesso a ferramentas e conhecimentos que podem apoiar o sucesso e a integridade operacional das AWS soluções. Além disso, considere se sua organização se beneficiaria com o uso de um Suporte plano AWS Managed Services em vez de usá-lo. [AWS Managed Services \(AMS\)](#) ajuda você a operar com mais eficiência e segurança fornecendo gerenciamento contínuo de sua AWS infraestrutura, incluindo monitoramento, gerenciamento de incidentes, orientação de segurança, suporte a patches e backup para AWS cargas de trabalho. O modelo de suporte do AMS pode ser mais adequado para organizações que têm recursos limitados em suas equipes de operações em nuvem. Recomendamos que você compare esses modelos e planos para escolher o mais adequado ao caso de uso e ao nível de maturidade da nuvem da sua organização.

Para obter mais informações, consulte os seguintes recursos:

- [Entenda as equipes de AWS resposta e o suporte](#) no Guia de Resposta a Incidentes de AWS Segurança
- [Atualize os contatos alternativos para você Conta da AWS](#) no Guia de gerenciamento de AWS contas
- [Compare Suporte os planos](#) no AWS site

- [Estratégia AWS Managed Services a ser usada para alcançar os resultados comerciais desejados](#) na Orientação AWS Prescritiva

Configurar alertas para eventos de segurança

Detectar uma anormalidade é tão importante quanto as medidas implementadas para controlar essa anormalidade. Um alerta é o principal componente da fase de detecção. Ele gera uma notificação para iniciar o processo de resposta a incidentes com base na Conta da AWS atividade de interesse. Certifique-se de que os alertas incluam informações relevantes para a equipe agir.

Para obter mais informações, consulte os seguintes recursos:

- [Detecção](#) no Guia de Resposta a Incidentes de AWS Segurança
- [Prepare recursos forenses](#) no AWS Well-Architected Framework
- [Implemente eventos de segurança acionáveis](#) no AWS Well-Architected Framework

Próximas etapas

À medida que você continua sua jornada na nuvem, é importante aplicar esses controles, orientações e opções de remediação documentados. Essas recomendações ajudam a melhorar sua postura de segurança na nuvem e a cumprir suas responsabilidades de segurança no Nuvem AWS, conforme definido no modelo de responsabilidade AWS compartilhada.

Para as próximas etapas, recomendamos o seguinte:

- Para obter mais informações sobre as melhores práticas e diretrizes de implementação, revise os seis pilares do [AWS Well-Architected](#) Framework.
- Para o Serviços da AWS que sua organização usa, revise a lista de [AWS Security Hub controles](#) disponíveis e avalie se você deve habilitar algum desses controles em seu ambiente.
- Para o Serviços da AWS que sua organização usa, revise a lista de [regras AWS Config gerenciadas](#) disponíveis e avalie se você deve habilitar alguma dessas regras em seu ambiente.

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
MFA para usuário root	Atualizamos as recomendações e fornecemos mais informações na seção MFA para o usuário raiz .	9 de novembro de 2023
Publicação inicial	—	27 de outubro de 2023

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migre seu banco de dados Oracle local para a edição compatível com 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 EC2 instância no. Nuvem AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma local para um serviço em nuvem para a mesma plataforma. Exemplo: migrar um Microsoft Hyper-V aplicativo para AWS.
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.

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

A

ABAC

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

serviços abstratos

Veja os [serviços gerenciados](#).

ACID

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

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja a [inteligência artificial](#).

AIOps

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

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade (ACID)

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

controle de acesso 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.

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 em nuvem (CCoE)

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

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

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

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação — Fazer investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma landing zone, definir um CCo E, 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 or Bitbucket Cloud. 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 AI 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. CI/CD is commonly described as a pipeline. CI/CD pode ajudá-lo 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

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

design orientado por domínio

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

DR

Veja a [recuperação de desastres](#).

detecção de deriva

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

DVSM

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

E

EDA

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

EDI

Veja [intercâmbio eletrônico 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.

intercâmbio eletrônico de dados (EDI)

A troca automatizada de documentos comerciais entre organizações. Para obter mais informações, consulte [O que é intercâmbio eletrônico de dados](#).

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).

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 do 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

Veja o [planejamento de recursos corporativos](#).

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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.

solicitação de alguns instantes

Fornecer a um [LLM](#) um pequeno número de exemplos que demonstram a tarefa e o resultado desejado antes de solicitar que ele execute uma tarefa semelhante. Essa técnica é uma aplicação do aprendizado contextual, em que os modelos aprendem com exemplos (fotos) incorporados aos prompts. Solicitações rápidas podem ser eficazes para tarefas que exigem formatação, raciocínio ou conhecimento de domínio específicos. Veja também a solicitação [zero-shot](#).

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.

FM

Veja o [modelo da fundação](#).

modelo de fundação (FM)

Uma grande rede neural de aprendizado profundo que vem treinando em grandes conjuntos de dados generalizados e não rotulados. FMs são capazes de realizar uma ampla variedade de tarefas gerais, como entender a linguagem, gerar texto e imagens e conversar em linguagem natural. Para obter mais informações, consulte [O que são modelos básicos](#).

G

IA generativa

Um subconjunto de modelos de [IA](#) que foram treinados em grandes quantidades de dados e que podem usar uma simples solicitação de texto para criar novos conteúdos e artefatos, como imagens, vídeos, texto e áudio. Para obter mais informações, consulte [O que é IA generativa](#).

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.

imagem dourada

Um instantâneo de um sistema ou software usado como modelo para implantar novas instâncias desse sistema ou software. Por exemplo, na manufatura, uma imagem dourada pode ser usada para provisionar software em vários dispositivos e ajudar a melhorar a velocidade, a escalabilidade e a produtividade nas operações de fabricação de dispositivos.

estratégia greenfield

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

barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais (OU)s. 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.

dados de retenção

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de aprendizado [de máquina](#). Você pode usar dados de retenção para avaliar o desempenho do modelo comparando as previsões do modelo com os dados de retenção.

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

eu

laC

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 AWS Segurança](#) recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

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 AWS Segurança](#) recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

Internet das Coisas (IoT)

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

interpretabilidade

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

IoT

Consulte [Internet das Coisas](#).

Biblioteca de informações de TI (ITIL)

Um conjunto de práticas recomendadas para fornecer serviços de TI e alinhar esses serviços a requisitos de negócios. 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](#).

modelo de linguagem grande (LLM)

Um modelo de [IA](#) de aprendizado profundo que é pré-treinado em uma grande quantidade de dados. Um LLM pode realizar várias tarefas, como responder perguntas, resumir documentos, traduzir texto para outros idiomas e completar frases. Para obter mais informações, consulte [O que são LLMs](#).

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

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

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja [7 Rs](#).

sistema little-endian

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

LLM

Veja [um modelo de linguagem grande](#).

ambientes inferiores

Veja o [ambiente](#).

M

machine learning (ML)

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

ramificação principal

Veja a [filial](#).

malware

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

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte [Migration Acceleration Program](#).

mecanismo

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

conta de membro

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

MES

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

Transporte de telemetria de enfileiramento de mensagens (MQTT)

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

microsserviço

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

arquitetura de microsserviços

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

de uma interface bem definida usando leveza. APIs Cada 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 a Amazon EC2 com o AWS 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 todas as 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.

ORR

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

OT

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 AWS Segurança](#) recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja as [informações de identificação pessoal](#).

manual

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

PLC

Consulte [controlador lógico programável](#).

AMEIXA

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

política

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

persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um microserviço com base em padrões de acesso a dados e outros requisitos. Se seus microserviços tiverem a mesma tecnologia de armazenamento de dados, eles poderão enfrentar desafios de implementação ou apresentar baixa performance. Os microserviços 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 microserviços](#).

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 de engenharia de sistema que leva em consideração a privacidade em todo o processo de desenvolvimento.

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja o [ambiente](#).

controlador lógico programável (PLC)

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

encadeamento imediato

Usando a saída de um prompt do [LLM](#) como entrada para o próximo prompt para gerar respostas melhores. Essa técnica é usada para dividir uma tarefa complexa em subtarefas ou para refinar ou expandir iterativamente uma resposta preliminar. Isso ajuda a melhorar a precisão e a relevância das respostas de um modelo e permite resultados mais granulares e personalizados.

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.

publish/subscribe (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

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

RAG

Consulte [Geração Aumentada de Recuperação](#).

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](#).

Geração Aumentada de Recuperação (RAG)

Uma tecnologia de [IA generativa](#) na qual um [LLM](#) faz referência a uma fonte de dados autorizada que está fora de suas fontes de dados de treinamento antes de gerar uma resposta. Por exemplo, um modelo RAG pode realizar uma pesquisa semântica na base de conhecimento ou nos dados personalizados de uma organização. Para obter mais informações, consulte [O que é RAG](#).

alternância

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.

segurança por design

Uma abordagem de engenharia de sistema que leva em consideração a segurança em todo o processo de desenvolvimento.

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 EC2 da Amazon ou a rotação de credenciais.

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização em AWS Organizations. SCPs defina barreiras ou estabeleça limites nas ações que um administrador pode delegar a usuários ou funções. Você pode usar SCPs como listas de permissão ou listas de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte [Políticas de controle de serviço](#) na AWS Organizations documentação.

service endpoint (endpoint de serviço)

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

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. Cada sub-rede fica alocada em uma única zona de disponibilidade.

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

prompt do sistema

Uma técnica para fornecer contexto, instruções ou diretrizes a um [LLM](#) para direcionar seu comportamento. Os prompts do sistema ajudam a definir o contexto e estabelecer regras para interações com os usuários.

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o [ambiente](#).

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

Uma abordagem na qual os desenvolvedores criam e testam recursos localmente em uma ramificação de recursos e, em seguida, mesclam essas alterações na ramificação principal. A

ramificação principal é então criada para os ambientes de desenvolvimento, pré-produção e produção, sequencialmente.

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o [ambiente](#).

V

aspiração

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

controle de versões

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

emparelhamento da VPC

Uma conexão entre duas VPCs que permite rotear o 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 [Estrutura de qualificação AWS da carga de trabalho](#).

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.

aviso zero-shot

Fornecer a um [LLM](#) instruções para realizar uma tarefa, mas sem exemplos (fotos) que possam ajudar a orientá-la. O LLM deve usar seu conhecimento pré-treinado para lidar com a tarefa. A

eficácia da solicitação zero depende da complexidade da tarefa e da qualidade da solicitação.
Veja também a solicitação [de algumas fotos](#).

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.