



Alcançando a maturidade do Essential AWS

AWS Orientação prescritiva



AWS Orientação prescritiva: Alcançando a maturidade do Essential AWS

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 desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

Introdução	1
Segurança e conformidade australianas	2
Programa de avaliadores registrados de segurança da informação	2
Estrutura de certificação de hospedagem	2
AWS modelo de responsabilidade compartilhada	3
AWS Estrutura Well-Architected	3
Reinterpretando as oito estratégias essenciais	4
Usando os temas	5
Reinterpretando as oito estratégias essenciais para a nuvem	5
Quais serviços você está usando?	5
Qual modelo de implantação você está usando?	6
Tema 1: Serviços gerenciados	8
Práticas recomendadas relacionadas:	9
Implementando este tema	9
Ativar a aplicação de patches	9
Verifique se há vulnerabilidades	9
Monitorando este tema	10
Implemente verificações de controle	10
Monitore o Amazon Inspector	10
Implemente as seguintes AWS Config regras	10
Tema 2: Infraestrutura imutável	11
Práticas recomendadas relacionadas:	12
Implementando este tema	12
Implemente a AMI e os pipelines de construção de contêineres	12
Implemente pipelines seguros de criação de aplicativos	13
Implementar verificação de vulnerabilidades	13
Monitorando este tema	14
Monitore o IAM e os registros continuamente	14
Implemente as seguintes AWS Config regras	14
Tema 3: Infraestrutura mutável	15
Práticas recomendadas relacionadas:	15
Implementando este tema	16
Automatize a aplicação de patches	16
Use automação em vez de processos manuais	16

Use a automação para instalar o seguinte nas EC2 instâncias	16
Use a revisão por pares antes de qualquer lançamento para garantir que as mudanças estejam de acordo com as melhores práticas	16
Use controles em nível de identidade	17
Implementar verificação de vulnerabilidades	17
Monitorando este tema	17
Monitore a conformidade dos patches continuamente	17
Monitore o IAM e os registros continuamente	17
Implemente as seguintes AWS Config regras	18
Tema 4: Identidades	19
Práticas recomendadas relacionadas:	20
Implementando este tema	20
Implementar federação de identidade	20
Aplicar permissões de privilégio mínimo	20
Alterne as credenciais	21
Aplique o MFA	21
Monitorando este tema	21
Monitore o acesso com privilégios mínimos	21
Implemente as seguintes AWS Config regras	22
Tema 5: Perímetro de dados	23
Práticas recomendadas relacionadas:	23
Implementando este tema	24
Implemente controles de identidade	24
Implemente controles de recursos	24
Implemente controles de rede	24
Monitorando este tema	25
Monitorar políticas	25
Implemente as seguintes AWS Config regras	25
Tema 6: Backups	26
Melhores práticas relacionadas no AWS Well-Architected Framework	27
Implementando este tema	27
Automatize o backup e a recuperação de dados	27
Práticas recomendadas relacionadas:	27
Monitorando este tema	27
Implemente as seguintes AWS Config regras	27
Tema 7: Registro e monitoramento	29

Práticas recomendadas relacionadas:	30
Implementando este tema	30
Habilitar registro em log	30
Implemente as melhores práticas de segurança de registro	30
Centralize os registros	30
Monitorando este tema	31
Implementar mecanismos	31
Implemente as seguintes AWS Config regras	31
Tema 8: Mecanismos para processos manuais	32
Práticas recomendadas relacionadas:	32
Implementando este tema	33
Monitorando este tema	33
Estudo de caso	34
Visão geral	34
Arquitetura principal	34
Data lake sem servidor	35
Serviço web em contêineres	37
Software COTS	39
Recursos	42
AWS documentação	42
Outros AWS recursos	42
Recursos do Australian Cyber Security Center	42
Colaboradores	43
Apêndice: Matrizes de controle	44
Controle de aplicativos	44
Aplicativos de patch	49
Configurar Microsoft Office configurações de macro	58
Fortalecimento de aplicativos do usuário	61
Restringir privilégios administrativos	63
Patch de sistemas operacionais	72
Autenticação multifator	78
Backups regulares	83
Avisos	85
Histórico do documento	86
Glossário	87
#	87

A	88
B	91
C	93
D	96
E	100
F	102
G	104
H	105
eu	107
L	109
M	110
O	115
P	117
Q	120
R	121
S	124
T	128
U	129
V	130
W	130
Z	131
.....	cxviii

Alcançando a maturidade da Essential Eight em AWS: Segurança e conformidade para organizações australianas

Amazon Web Services ([colaboradores](#))

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

A Australian Signals Directorate (ASD) criou e priorizou estratégias para ajudar as organizações a mitigar os riscos das ameaças à segurança cibernética. Oito dessas estratégias foram escolhidas para formar a estrutura Essential Eight. Muitas organizações do setor público e privado na Austrália precisam atingir a maturidade de acordo com a estrutura Essential Eight.

O Australian Cyber Security Centre (ACSC) criou a estrutura Essential Eight para ajudar a proteger Microsofts conectadas à Internet baseadas na Internet. No entanto, muitas organizações precisam atingir a maturidade do Essential Eight para todos os seus ambientes, tanto no local quanto na nuvem.

A estrutura Essential Eight também inclui um [modelo de maturidade](#) projetado para ajudar as organizações a implementar a estrutura por meio de iteração progressiva. O modelo descreve os níveis de maturidade de zero a três. O nível de maturidade três representa resiliência contra táticas avançadas de cibersegurança e ataques altamente direcionados. Este guia fornece orientação específica e opinativa para ajudá-lo a atingir o nível três de maturidade do Essential Eight. AWS

Segurança e conformidade para organizações australianas

Muitas organizações na Austrália usam Nuvem AWS o para armazenar dados confidenciais, processar transações confidenciais e criar serviços essenciais.

Embora este guia discuta como adaptar a estrutura Essential Eight para a nuvem, AWS também fornece as seguintes certificações e modelos para ajudá-lo a atender aos requisitos de segurança e conformidade da sua organização:

- [Programa de avaliadores registrados de segurança da informação](#)
- [Estrutura de certificação de hospedagem](#)
- [AWS modelo de responsabilidade compartilhada](#)
- [AWS Estrutura Well-Architected](#)

Programa de avaliadores registrados de segurança da informação

Serviços da AWS foram avaliados pelo [Programa de Avaliadores Registrados de Segurança da Informação \(IRAP\) do Australian Cyber Security Centre \(ACSC\)](#) no nível PROTECTED. Um avaliador independente do IRAP certificado pela Australian Signals Directorate (ASD) concluiu a avaliação do IRAP de. AWS Essa avaliação garante que, com relação aos AWS produtos e serviços, os controles aplicáveis sejam implementados para cargas de trabalho de nível PROTEGIDO.

O pacote AWS IRAP PROTECTED está disponível em. [AWS Artifact](#) O relatório do IRAP foi desenvolvido usando a [orientação de segurança do ACSC Cloud](#) (site do ACSC). Para obter uma lista completa dos Serviços da AWS que estão no escopo, consulte [Serviços da AWS no escopo: IRAP](#).

Estrutura de certificação de hospedagem

A [Estrutura de Certificação de Hospedagem](#) Australiana foi desenvolvida para apoiar o gerenciamento seguro de sistemas e dados governamentais. Essa estrutura tem como objetivo ajudar as organizações a mitigar os riscos de propriedade da cadeia de suprimentos e do data center. AWS recebeu a certificação no nível Estratégico Certificado. Isso ajuda as agências governamentais a continuarem inovando em um ritmo acelerado, sabendo que AWS atende aos requisitos governamentais.

AWS modelo de responsabilidade compartilhada

O [modelo de responsabilidade AWS compartilhada](#) define como você compartilha a responsabilidade AWS pela segurança e conformidade na nuvem. AWS protege a infraestrutura que executa todos os serviços oferecidos no Nuvem AWS, e você é responsável por proteger o uso desses serviços, como seus dados e aplicativos.

Esse modelo compartilhado pode ajudar a aliviar sua carga operacional e de conformidade porque AWS opera, gerencia e controla muitos componentes, desde o sistema operacional do host e a camada de virtualização até a segurança física das instalações nas quais o serviço opera. Você assume a responsabilidade pelo gerenciamento do sistema operacional convidado (incluindo atualizações e patches de segurança) e outros softwares de aplicativos associados. Você também assume a responsabilidade pela configuração do firewall do grupo de segurança que AWS fornece.

É fundamental que você entenda o modelo de responsabilidade AWS compartilhada ao abordar a maturidade do Essential Eight em AWS. Suas responsabilidades variam de acordo com os serviços usados, a integração desses serviços em seu ambiente de TI e as leis e regulamentações aplicáveis.

AWS Estrutura Well-Architected

AWS O Well-Architected ajuda os arquitetos de nuvem a criar uma infraestrutura segura, de alto desempenho, resiliente e eficiente para uma variedade de aplicativos e cargas de trabalho. O [AWS Well-Architected](#) Framework fornece as melhores práticas arquitetônicas que ajudam você a projetar, criar e operar sistemas em. AWS Essa estrutura é construída em torno de seis pilares: excelência operacional, segurança, confiabilidade, eficiência de desempenho, otimização de custos e sustentabilidade.

AWS também fornece um serviço para revisar suas cargas de trabalho. [AWS Well-Architected Tool](#) Isso ajuda você a revisar e avaliar sua arquitetura usando o AWS Well-Architected Framework. Ele fornece recomendações para tornar suas cargas de trabalho mais confiáveis, seguras, eficientes e econômicas.

Reinterpretando as oito estratégias essenciais para a nuvem

A seguir estão as estratégias originais de mitigação do Essential Eight que foram projetadas para Microsoft redes conectadas à Internet baseadas na Internet:

- Controle de aplicativos
- Aplicativos de patch
- Configurar Microsoft Office configurações de macro
- Fortalecimento de aplicativos do usuário
- Restringir privilégios administrativos
- Patch de sistemas operacionais
- Autenticação multifator
- Backups regulares

É importante reiterar que a estrutura Essential Eight não foi projetada para ambientes em nuvem. No entanto, os princípios subjacentes são aplicáveis e há uma sobreposição entre as estratégias Essential Eight e as melhores práticas do AWS Well-Architected Framework.

Várias abordagens nativas da nuvem podem melhorar a segurança e reduzir drasticamente sua carga de conformidade. Em ambientes locais, você é responsável por todos os aspectos da segurança e não há controles herdados. Ao executar cargas de trabalho na nuvem, AWS é responsável por proteger a infraestrutura que executa nossos serviços. Você também pode reduzir sua carga de conformidade usando automação e serviços gerenciados. Os serviços gerenciados, também conhecidos como serviços abstratos, AWS operam a camada de infraestrutura, o sistema operacional e as plataformas, e você acessa os endpoints para armazenar e recuperar dados. Serviços da AWS O Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB são exemplos de serviços gerenciados. Para obter mais informações, consulte a [Tema 1: Usar serviços gerenciados](#) seção deste guia.

Portanto, alguma reinterpretação é necessária para tornar as estratégias Essential Eight apropriadas para cargas de trabalho em AWS. Este guia converte as estratégias Essential Eight em AWS temas.

Usando os temas

Este guia está dividido em oito temas. Cada estratégia do Essential Eight é mapeada para um ou mais dos seguintes temas, e cada tema é mapeado para uma ou mais melhores práticas no Well-Architected AWS Framework:

- [Tema 1: Usar serviços gerenciados](#)
- [Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras](#)
- [Tema 3: Gerenciar infraestrutura mutável com automação](#)
- [Tema 4: Gerenciar identidades](#)
- [Tema 5: Estabelecer um perímetro de dados](#)
- [Tema 6: Automatizar backups](#)
- [Tema 7: Centralizar o registro e o monitoramento](#)
- [Tema 8: Implementar mecanismos para processos manuais](#)

Cada tema inclui uma visão geral do tópico, as melhores práticas relacionadas ao AWS Well-Architected Framework e instruções sobre como alcançar a maturidade do Essential Eight e monitorar a conformidade. As instruções fornecem etapas manuais ou ajudam você a configurar automações usando [AWS Config regras](#). As etapas manuais exigem mecanismos para garantir que as descobertas sejam abordadas. Para obter mais informações, consulte [Tema 8: Implementar mecanismos para processos manuais](#). AWS Config as regras exigem supervisão ou automação semelhantes para [remediar recursos não compatíveis](#). Seguindo as orientações alinhadas a esses temas, você pode alcançar a maturidade do Essential Eight com uma abordagem que também maximiza os benefícios da nuvem.

Reinterpretando as oito estratégias essenciais para a nuvem

Como a estrutura do Essential Eight não foi projetada para ambientes de nuvem, é essencial adotar uma abordagem nativa da nuvem ao abordar os princípios subjacentes de cada estratégia do Essential Eight. A abordagem varia de acordo com duas questões principais.

Quais serviços você está usando?

Eles [AWS modelo de responsabilidade compartilhada](#) podem ajudar a aliviar seus encargos operacionais e de conformidade. Os serviços gerenciados transferem mais responsabilidade AWS

para manter a disponibilidade, o desempenho e a otimização da segurança do serviço implantado. Os serviços gerenciados também eliminam a carga operacional e administrativa de manter um serviço, oferecendo mais tempo para se concentrar na inovação.

Os serviços gerenciados incluem serviços sem servidor, como Amazon API Gateway e DynamoDB. AWS Lambda Um banco de dados no Amazon Relational Database Service (Amazon RDS) exige menos responsabilidade operacional do que um banco de dados no Amazon Elastic Compute Cloud (Amazon). EC2

Por exemplo, se você estiver adaptando a estratégia Essential Eight dos sistemas operacionais Patch para a nuvem, precisará considerar quais serviços está usando e se é responsável por corrigir esses recursos. AWS é responsável por corrigir serviços totalmente gerenciados, como Lambda e DynamoDB. Para outros serviços, como Amazon RDS ou Amazon Redshift, talvez seja necessário gerenciar patches durante as janelas de manutenção.

Qual modelo de implantação você está usando?

Sua organização está usando uma abordagem de infraestrutura mutável ou imutável?

O modelo de infraestrutura mutável atualiza e modifica a infraestrutura existente para cargas de trabalho de produção. Esse era o método padrão de implantação antes da nuvem, quando a substituição da infraestrutura do servidor era tão cara e demorada que a abordagem mais prática era aplicar alterações nos servidores que já estavam em produção. Um exemplo de abordagem mutável na nuvem é implantar alterações de aplicativos diretamente nas EC2 instâncias em execução, manualmente ou usando um serviço de implantação de software, como AWS Systems Manager Run Command ou. AWS CodeDeploy

O modelo de infraestrutura imutável implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. Um exemplo de abordagem imutável é definir uma pilha de aplicativos em ou. AWS CloudFormationAWS Cloud Development Kit (AWS CDK) Você pode usar esses serviços para implantar uma pilha de aplicativos por meio de pipelines de integração contínua e entrega contínua (CI/CD). Essa abordagem usa métodos de implantação, como rolagem ou azul/verde. Para obter mais informações sobre essa abordagem, consulte as melhores práticas de implantação usando infraestrutura imutável no Well-Architected AWS Framework.

Por exemplo, se você estiver adaptando a estratégia Essential Eight dos sistemas operacionais Patch para a nuvem, precisará considerar como os patches se aplicam ao modelo de implantação. Para uma infraestrutura mutável, você pode corrigir recursos manualmente ou melhorar a eficiência

operacional por meio da automação. Se você estiver usando uma infraestrutura imutável, use um pipeline de CI/CD para implantar uma nova infraestrutura com a versão mais recente do sistema operacional. Na verdade, o termo patch é um termo impróprio nesse modelo porque a infraestrutura seria substituída em vez de corrigida.

Tema 1: Usar serviços gerenciados

Oito estratégias essenciais abordadas

Corrija aplicativos, restrinja privilégios administrativos, corrija sistemas operacionais

Os serviços gerenciados ajudam você a reduzir suas obrigações de conformidade, AWS permitindo gerenciar algumas tarefas de segurança, como correção e gerenciamento de vulnerabilidades.

Conforme discutido na [AWS modelo de responsabilidade compartilhada](#) seção, você compartilha a responsabilidade pela segurança e conformidade na nuvem. AWS Isso pode reduzir sua carga operacional porque AWS opera, gerencia e controla componentes, desde o sistema operacional host e a camada de virtualização até a segurança física das instalações nas quais o serviço opera.

Suas responsabilidades podem incluir o gerenciamento de janelas de manutenção para serviços gerenciados, como o Amazon Relational Database Service (Amazon RDS) ou o Amazon Redshift, e a verificação de vulnerabilidades AWS Lambda em imagens de código ou contêiner. Como em todos os temas deste guia, você também é responsável pelo monitoramento e pelos relatórios de conformidade. Você pode usar o [Amazon Inspector](#) para relatar vulnerabilidades em todos os seus. Contas da AWS Você pode usar regras AWS Config para garantir que serviços, como Amazon RDS e Amazon Redshift, tenham pequenas atualizações e janelas de manutenção habilitadas.

Por exemplo, se você executa uma EC2 instância da Amazon, suas responsabilidades incluem o seguinte:

- Controle de aplicativos
- Aplicação de patches
- Restringindo privilégios administrativos ao plano EC2 de controle da Amazon e ao sistema operacional (OS)
- Corrigindo o sistema operacional
- Aplicação da autenticação multifatorial (MFA) para acessar o plano de AWS controle e o sistema operacional
- Fazendo backup dos dados e da configuração

Por outro lado, se você executa uma função Lambda, suas responsabilidades são reduzidas e incluem o seguinte:

- Controle de aplicativos
- Confirmando que as bibliotecas são up-to-date
- Restringindo privilégios administrativos ao plano de controle Lambda
- Aplicando o MFA para acessar o plano de controle AWS
- Fazendo backup do código e da configuração da função Lambda

Melhores práticas relacionadas no AWS Well-Architected Framework

- [SEC01-BP05 Reduza o escopo do gerenciamento de segurança](#)

Implementando este tema

Ativar a aplicação de patches

- [Aplique atualizações do Amazon RDS](#)
- [Ativar atualizações gerenciadas em AWS Elastic Beanstalk](#)
- [Esteja ciente das janelas de manutenção de clusters do Amazon Redshift](#)

Verifique se há vulnerabilidades

- [Digitalize imagens de contêineres do Amazon Elastic Container Registry \(Amazon ECR\) com o Amazon Inspector](#)
- [Digitalize as funções do Lambda com o Amazon Inspector](#)

Monitorando este tema

Implemente verificações de controle

- Ative as [melhores práticas operacionais para o pacote de conformidade do ACSC Essential 8](#) em AWS Config

Monitore o Amazon Inspector

- [Avalie a cobertura em nível de conta](#)
- [Gerencie várias contas](#)

Implemente as seguintes AWS Config regras

- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EKS_CLUSTER_SUPPORTED_VERSION

Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras

Oito estratégias essenciais abordadas

Controle de aplicativos, aplicativos de patches, sistemas operacionais de patches

Para uma infraestrutura imutável, você deve proteger os pipelines de implantação para alterações no sistema. AWS O ilustre engenheiro, Colm MacCárthaigh, explicou esse princípio em Operações com [privilegio zero](#): execução de serviços sem acesso aos dados (YouTube vídeo) apresentação na conferência AWS re:Invent de 2022.

Ao restringir o acesso direto para configurar AWS recursos, você pode exigir que todos os recursos sejam implantados ou alterados por meio de pipelines aprovados, protegidos e automatizados. Normalmente, você cria políticas [AWS Identity and Access Management \(IAM\)](#) que permitem que os usuários acessem somente a conta que hospeda o pipeline de implantação. Você também configura políticas do IAM que [permitem acesso rápido](#) a um número limitado de usuários. Para evitar alterações manuais, você pode usar grupos de segurança para bloquear SSH e Windows acesso ao protocolo de desktop remoto (RDP) aos servidores. O [Gerenciador de Sessões](#) AWS Systems Manager, um recurso do, pode fornecer acesso às instâncias sem a necessidade de abrir portas de entrada ou manter os bastion hosts.

Amazon Machine Images (AMIs) e imagens de contêiner devem ser criadas de forma segura e repetitiva. Para EC2 instâncias da Amazon, você pode usar o [EC2 Image Builder](#) para criar AMIs que tenham recursos de segurança integrados, como descoberta de instâncias, controle de aplicativos e registro em log. Para obter mais informações sobre o controle de aplicativos, consulte [Implementando o controle de aplicativos](#) no site do ACSC. Você também pode usar o Image Builder para criar imagens de contêineres e usar o [Amazon Elastic Container Registry \(Amazon ECR\)](#) para compartilhar essas imagens entre contas. Uma equipe de segurança central pode aprovar o processo automatizado para criar essas imagens AMIs e as imagens de contêiner para que qualquer AMI ou imagem de contêiner resultante seja aprovada para uso pelas equipes de aplicativos.

Os aplicativos devem ser definidos na infraestrutura como código (IaC), usando serviços como [AWS CloudFormation](#) ou [AWS Cloud Development Kit \(AWS CDK\)](#). Ferramentas de análise de código AWS CloudFormation Guard, como cfn-nag ou cdk-nag, podem testar automaticamente o código de acordo com as melhores práticas de segurança em seu pipeline aprovado.

Assim como acontece com [Tema 1: Usar serviços gerenciados](#), o Amazon Inspector pode relatar vulnerabilidades em todo o seu. Contas da AWS As equipes centralizadas de nuvem e segurança podem usar essas informações para verificar se a equipe de aplicativos está atendendo aos requisitos de segurança e conformidade.

Para monitorar e relatar a conformidade, realize análises contínuas dos recursos e registros do IAM. Use AWS Config regras para garantir que somente AMIs os aprovados sejam usados e certifique-se de que o Amazon Inspector esteja configurado para verificar se há vulnerabilidades nos recursos do Amazon ECR.

Melhores práticas relacionadas no AWS Well-Architected Framework

- [OPS05-BP04 Usar sistemas de gerenciamento de compilação e implantação](#)
- [REL08-BP04 Implantar usando infraestrutura imutável](#)
- [SEC06-BP03 Reduzir o gerenciamento manual e o acesso interativo](#)

Implementando este tema

Implemente a AMI e os pipelines de construção de contêineres

- [Use o EC2 Image Builder](#) e inclua o seguinte em seu AMIs:
 - [AWS Systems Manager Agente \(Agente SSM\)](#), que é usado para descoberta e gerenciamento de instâncias
 - [Ferramentas de segurança para controle de aplicativos, como Security Enhanced Linux \(SELinux\) \(GitHub\), File Access Policy Daemon \(fapolicyd\) \(\) ou OpenSCAP GitHub](#)
 - [Amazon CloudWatch Agent](#), que é usado para registro
- Para todas as EC2 instâncias, inclua AmazonSSMManagedInstanceCore as políticas CloudWatchAgentServerPolicy e no [perfil da instância ou na função do IAM](#) que o Systems Manager usa para acessar sua instância
- [Compartilhe AMIs com toda a organização](#)
- [Compartilhe recursos do EC2 Image Builder](#)
- [Certifique-se de que as equipes de aplicativos estejam referenciando as últimas AMIs](#)
- [Use seu pipeline de AMI para gerenciamento de patches](#)

- Implemente pipelines de construção de contêineres:
 - [Crie um pipeline de imagem de contêiner usando o assistente de console do EC2 Image Builder](#)
 - [Crie um pipeline de entrega contínua para suas imagens de contêiner usando o Amazon ECR como fonte](#) (postagem AWS no blog)
- [Compartilhe imagens de contêineres ECR em toda a sua organização por meio de arquiteturas multicontas e multirregiões](#)

Implemente pipelines seguros de criação de aplicativos

- Implemente pipelines de construção para IaC, por exemplo, usando [EC2 Image Builder e AWS CodePipeline](#) (AWS postagem no blog)
- Use ferramentas de análise de código [AWS CloudFormation Guard](#), como [cfn-nag \(GitHub\)](#) ou [cdk-nag](#) (GitHub), em pipelines de CI/CD para ajudar a detectar violações das melhores práticas, como:
 - Políticas do IAM que são muito permissivas, como aquelas que usam curingas
 - Regras de grupo de segurança que são muito permissivas, como aquelas que usam curingas ou permitem acesso SSH
 - Registros de acesso que não estão habilitados
 - Criptografia que não está ativada
 - Literais de senha
- [Implemente ferramentas de digitalização em pipelines](#) (postagem AWS no blog)
- [Use AWS Identity and Access Management Access Analyzer em pipelines](#) (postagem AWS do blog) para validar políticas do IAM definidas em modelos CloudFormation
- Configure [políticas do IAM](#) e [políticas de controle de serviços](#) para acesso com privilégios mínimos para usar o pipeline ou fazer modificações nele

Implementar verificação de vulnerabilidades

- [Habilite o Amazon Inspector em todas as contas da sua organização](#)
- Use o Amazon Inspector para escanear seu pipeline AMIs de criação de AMI:
 - [Gerencie o ciclo de vida do AMIs no EC2 Image Builder](#) () GitHub
- [Configure a digitalização aprimorada para repositórios do Amazon ECR usando o Amazon Inspector](#)

- [Crie um programa de gerenciamento de vulnerabilidades para fazer a triagem e corrigir as descobertas de segurança](#)

Monitorando este tema

Monitore o IAM e os registros continuamente

- Revise periodicamente suas políticas do IAM para garantir que:
 - Somente os pipelines de implantação têm acesso direto aos recursos
 - Somente serviços aprovados têm acesso direto aos dados
 - Os usuários não têm acesso direto a recursos ou dados
- Monitore AWS CloudTrail os registros para confirmar se os usuários estão modificando recursos por meio de pipelines e não estão modificando recursos ou acessando dados diretamente
- Analise periodicamente as descobertas do IAM Access Analyzer
- Configure um alerta para notificá-lo se as credenciais do usuário raiz de um Conta da AWS forem usadas

Implemente as seguintes AWS Config regras

- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED

Tema 3: Gerenciar infraestrutura mutável com automação

Oito estratégias essenciais abordadas

Controle de aplicativos, aplicativos de patches, sistemas operacionais de patches

Semelhante à infraestrutura imutável, você gerencia a infraestrutura mutável como IaC e modifica ou atualiza essa infraestrutura por meio de processos automatizados. Muitas das etapas de implementação da infraestrutura imutável também se aplicam à infraestrutura mutável. No entanto, para uma infraestrutura mutável, você também deve implementar controles manuais para garantir que as cargas de trabalho modificadas ainda sigam as melhores práticas.

Para uma infraestrutura mutável, você pode automatizar o gerenciamento de patches usando o [Patch Manager](#), um recurso de. AWS Systems Manager Ative o Patch Manager em todas as contas AWS da sua organização.

Evite o acesso direto ao SSH e ao RDP e exija que os usuários usem o [Session Manager](#) ou o [Run Command](#), que também são recursos do Systems Manager. Diferentemente do SSH e do RDP, esses recursos podem registrar o acesso e as alterações do sistema.

Para monitorar e relatar a conformidade, você deve realizar análises contínuas da conformidade do patch. Você pode usar AWS Config regras para garantir que todas as EC2 instâncias da Amazon sejam gerenciadas pelo Systems Manager, tenham as permissões necessárias e os aplicativos instalados e estejam em conformidade com os patches.

Melhores práticas relacionadas no AWS Well-Architected Framework

- [SEC06-BP03 Reduzir o gerenciamento manual e o acesso interativo](#)
- [SEC06-BP05 Automatize a proteção computacional](#)

Implementando este tema

Automatize a aplicação de patches

- Implemente as etapas em [Habilitar o Patch Manager em todas as contas AWS da sua organização](#)
- Para todas as EC2 instâncias, inclua CloudWatchAgentServerPolicy e AmazonSSMManagedInstanceCore no [perfil da instância ou na função do IAM](#) que o Systems Manager usa para acessar sua instância

Use automação em vez de processos manuais

- Implemente a orientação em [Implementar a AML e os pipelines de construção de contêineres](#) no [Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras](#)
- Use o [Gerenciador de Sessões](#) ou [Execute o Comando](#) em vez do acesso direto por SSH ou RDP

Use a automação para instalar o seguinte nas EC2 instâncias

- [AWS Systems Manager Agente \(Agente SSM\)](#), que é usado para descoberta e gerenciamento de instâncias
- [Ferramentas de segurança para controle de aplicativos, como Security Enhanced Linux \(SELinux\) \(GitHub\), File Access Policy Daemon \(fapolicyd\) \(\) ou OpenSCAP GitHub](#)
- [Amazon CloudWatch Agent](#), que é usado para registro

Use a revisão por pares antes de qualquer lançamento para garantir que as mudanças estejam de acordo com as melhores práticas

- Políticas do IAM que são muito permissivas, como aquelas que usam curingas
- Regras de grupo de segurança que são muito permissivas, como aquelas que usam curingas ou permitem acesso SSH
- Registros de acesso que não estão habilitados
- Criptografia que não está ativada
- Literais de senha
- Políticas seguras de IAM

Use controles em nível de identidade

- Para exigir que os usuários modifiquem recursos por meio de processos automatizados e evitar a configuração manual, conceda permissões somente de leitura para funções que os usuários possam assumir
- Conceda permissões para modificar recursos somente para funções de serviço, como a função usada pelo Systems Manager

Implementar verificação de vulnerabilidades

- Implemente a orientação em [Implementar a verificação de vulnerabilidades](#) em [Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras](#)
- Escaneie suas EC2 instâncias usando o Amazon Inspector

Monitorando este tema

Monitore a conformidade dos patches continuamente

- [Relate a conformidade de patches usando automação e painéis](#)
- Implemente um mecanismo para revisar os painéis para verificar a conformidade dos patches

Monitore o IAM e os registros continuamente

- Revise periodicamente suas políticas do IAM para garantir que:
 - Somente os pipelines de implantação têm acesso direto aos recursos
 - Somente serviços aprovados têm acesso direto aos dados
 - Os usuários não têm acesso direto a recursos ou dados
- Monitore AWS CloudTrail os registros para garantir que os usuários estejam modificando recursos por meio de pipelines e não estejam modificando recursos ou acessando dados diretamente
- Revise periodicamente AWS Identity and Access Management Access Analyzer os resultados
- Configure um alerta para notificá-lo se as credenciais do usuário raiz de um Conta da AWS forem usadas

Implemente as seguintes AWS Config regras

- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED - SELinux/fapolicyd/OpenSCAP, CW Agent
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED - any unsupported apps
- IAM_ROLE_MANAGED_POLICY_CHECK - CW Logs, SSM
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC - 22, 3389

Tema 4: Gerenciar identidades

Oito estratégias essenciais abordadas

Restrinja privilégios administrativos, autenticação multifatorial

O gerenciamento robusto de identidade e permissões é um aspecto essencial do gerenciamento da segurança na nuvem. Práticas de identidade fortes equilibram o acesso necessário e o mínimo de privilégios. Isso ajuda as equipes de desenvolvimento a se moverem rapidamente sem comprometer a segurança.

Use a federação de identidades para centralizar o gerenciamento de identidades. Isso facilita o gerenciamento do acesso em vários aplicativos e serviços porque você está gerenciando o acesso em um único local. Isso também ajuda você a implementar permissões temporárias e autenticação multifator (MFA).

Conceda aos usuários somente as permissões necessárias para realizar suas tarefas. AWS Identity and Access Management Access Analyzer pode validar políticas e verificar o acesso público e entre contas. Recursos como políticas de controle AWS Organizations de serviço (SCPs), condições de política do IAM, limites de permissões do IAM e conjuntos de AWS IAM Identity Center permissões podem ajudar você a configurar o [controle de acesso refinado](#) (FGAC).

Ao fazer qualquer tipo de autenticação, é melhor usar credenciais temporárias para reduzir ou eliminar riscos, como credenciais sendo divulgadas, compartilhadas ou roubadas inadvertidamente. Use funções do IAM em vez de usuários do IAM.

Use mecanismos de login robustos, como o MFA, para reduzir o risco de as credenciais de login serem divulgadas inadvertidamente ou serem facilmente adivinhadas. Exija MFA para o usuário raiz, e você também pode exigí-la em nível de federação. Se o uso de usuários do IAM for inevitável, aplique a MFA.

Para monitorar e relatar a conformidade, você deve trabalhar continuamente para reduzir as permissões, monitorar as descobertas do IAM Access Analyzer e remover recursos do IAM não utilizados. Use AWS Config regras para garantir que mecanismos de login fortes sejam aplicados, que as credenciais tenham vida curta e que os recursos do IAM estejam em uso.

Melhores práticas relacionadas no AWS Well-Architected Framework

- [SEC02-BP01 Use mecanismos de login robustos](#)
- [SEC02-BP02 Usar credenciais temporárias](#)
- [SEC02-BP03 Armazenar e usar segredos com segurança](#)
- [SEC02-BP04 Confiar em um provedor de identidades centralizado](#)
- [SEC02-BP05 Auditar e fazer a rotação das credenciais periodicamente](#)
- [SEC02-BP06 Utilizar grupos de usuários e atributos](#)
- [SEC03-BP01 Definir requisitos de acesso](#)
- [SEC03-BP02 Conceder acesso de privilégio mínimo](#)
- [SEC03-BP03 Estabelecer processo de acesso de emergência](#)
- [SEC03-BP04 Reduzir as permissões continuamente](#)
- [SEC03-BP05 Definir barreiras de proteção de permissões para sua organização](#)
- [SEC03-BP06 Gerenciar o acesso com base no ciclo de vida](#)
- [SEC03-BP07 Analisar o acesso público e entre contas](#)
- [SEC03-BP08 Compartilhar recursos com segurança em sua organização](#)

Implementando este tema

Implementar federação de identidade

- [Exija que usuários humanos se federem com um provedor de identidade para acessar AWS usando credenciais temporárias](#)
- [Implemente acesso elevado temporário aos seus AWS ambientes](#)

Aplicar permissões de privilégio mínimo

- [Proteja suas credenciais de usuário root e não as use para tarefas diárias](#)
- [Use o IAM Access Analyzer para gerar políticas de privilégios mínimos com base na atividade de acesso](#)

- [Verifique o acesso público e entre contas aos recursos com o IAM Access Analyzer](#)
- [Use o IAM Access Analyzer para validar suas políticas do IAM para obter permissões seguras e funcionais](#)
- [Estabeleça barreiras de permissões em várias contas](#)
- [Use limites de permissões para definir o máximo de permissões que uma política baseada em identidade pode conceder](#)
- [Use condições nas políticas do IAM para restringir ainda mais o acesso](#)
- [Analise e remova regularmente usuários, funções, permissões, políticas e credenciais não utilizados](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)
- [Use o recurso de conjuntos de permissões no IAM Identity Center](#)

Alterne as credenciais

- [Exija que as cargas de trabalho usem funções do IAM para acessar AWS](#)
- [Automatize a exclusão de funções do IAM não utilizadas](#)
- [Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo](#)

Aplique o MFA

- [Exigir MFA para o usuário raiz](#)
- [Exigir MFA por meio do IAM Identity Center](#)
- [Considere exigir a MFA para ações de API específicas do serviço](#)

Monitorando este tema

Monitore o acesso com privilégios mínimos

- [Envie as descobertas do IAM Access Analyzer para AWS Security Hub](#)
- [Considere configurar notificações para descobertas críticas do IAM Identity Center](#)
- [Analise regularmente os relatórios de credenciais de seu Contas da AWS](#)

Implemente as seguintes AWS Config regras

- ACCESS_KEYS_ROTATED
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- IAM_PASSWORD_POLICY
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Tema 5: Estabelecer um perímetro de dados

Oito estratégias essenciais abordadas

Restringir privilégios administrativos

Um perímetro de dados é um conjunto de barreiras preventivas em seu AWS ambiente que ajudam a garantir que somente identidades confiáveis acessem recursos confiáveis das redes esperadas. Essas grades de proteção servem como limites sempre ativos que ajudam a proteger seus dados em um amplo conjunto de recursos. Contas da AWS Essas grades de proteção em toda a organização não substituem seus controles de acesso refinados existentes. Em vez disso, eles ajudam a melhorar sua estratégia de segurança, garantindo que todos os usuários, funções e recursos AWS Identity and Access Management (IAM) sigam um conjunto de padrões de segurança definidos.

Você pode estabelecer um perímetro de dados usando políticas que impedem o acesso de fora dos limites de uma organização, normalmente criadas em. AWS Organizations As três principais condições de autorização de perímetro usadas para estabelecer um perímetro de dados são:

- Identidades confiáveis — Diretores (funções ou usuários do IAM) dentro de você Contas da AWS ou Serviços da AWS agindo em seu nome.
- Recursos confiáveis — Recursos que estão em você Contas da AWS ou são gerenciados Serviços da AWS agindo em seu nome.
- Redes esperadas — Seus data centers locais e nuvens privadas virtuais (VPCs) ou as redes que Serviços da AWS atuam em seu nome.

Considere implementar perímetros de dados entre ambientes de diferentes classificações de dados, como OFFICIAL : SENSITIVE ou PROTECTED, ou diferentes níveis de risco, como desenvolvimento, teste ou produção. Para obter mais informações, consulte [Criando um perímetro de dados em AWS](#) (AWS whitepaper) e [Estabelecendo um perímetro de dados em AWS: Visão geral](#) (AWS postagem do blog).

Melhores práticas relacionadas no AWS Well-Architected Framework

- [SEC03-BP05 Definir barreiras de proteção de permissões para sua organização](#)

- [SEC07-BP02 Aplique controles de proteção de dados com base na sensibilidade dos dados](#)

Implementando este tema

Implemente controles de identidade

- Permita que somente identidades confiáveis acessem seus recursos — Use [políticas baseadas em recursos com as](#) chaves de condição `aws:PrincipalOrgID` e `aws:PrincipalIsAWSService`. Isso permite que somente diretores de sua AWS organização e de AWS acessem seus recursos.
- Permita identidades confiáveis somente de sua rede — Use políticas de [endpoint de VPC](#) com as chaves de condição `aws:PrincipalOrgID` e `aws:PrincipalIsAWSService`. Isso permite que somente diretores de sua AWS organização e de AWS acessem serviços por meio de VPC endpoints.

Implemente controles de recursos

- Permita que suas identidades acessem somente recursos confiáveis — Use [políticas de controle de serviço \(SCPs\)](#) com a chave `aws:ResourceOrgID` de condição. Isso permite que suas identidades acessem somente recursos em sua AWS organização.
- Permita o acesso a recursos confiáveis somente da sua rede — Use políticas de VPC endpoint com a chave de condição `aws:ResourceOrgID`. Isso permite que suas identidades acessem serviços somente por meio de VPC endpoints que fazem parte da sua organização. AWS

Implemente controles de rede

- Permita que as identidades acessem recursos somente das redes esperadas — Use SCPs com as chaves de condição `aws:SourceIp`, `aws:SourceVpc`, `aws:SourceVpce`, e `aws:ViaAWSService`. Isso permite que suas identidades acessem recursos somente a partir de endereços IP esperados, VPCs, endpoints de VPC e por meio de Serviços da AWS.
- Permita o acesso aos seus recursos somente a partir das redes esperadas — Use políticas baseadas em recursos com as chaves de condição `aws:SourceIp`, `aws:SourceVpc`, `aws:SourceVpce`, `aws:ViaAWSService`, e `aws:PrincipalIsAWSService`. Isso permite o acesso aos seus recursos somente a partir dos endpoints de VPC esperados, VPCs esperados ou Serviços da AWS, por meio de ou quando a identidade de chamada é uma IP AWS service (Serviço da AWS).

Monitorando este tema

Monitorar políticas

- Implemente mecanismos de revisão SCPs, políticas de IAM e políticas de VPC endpoint

Implemente as seguintes AWS Config regras

- SERVICE_VPC_ENDPOINT_ENABLED

Tema 6: Automatizar backups

Oito estratégias essenciais abordadas

Backups regulares

“As falhas são um dado adquirido e tudo acabará falhando com o tempo: de roteadores a discos rígidos, de sistemas operacionais a unidades de memória que corrompem pacotes TCP, de erros transitórios a falhas permanentes. Isso é garantido, independentemente de você estar usando hardware da mais alta qualidade ou componentes de menor custo.” —[Werner Vogels, CTO da Amazon, All Things Distributed](#)

O backup e a recuperação de dados são uma parte essencial da confiabilidade de um sistema. AWS foi projetado para facilitar a criação de backups, manter a durabilidade dos dados de backup e garantir que os dados de backup permaneçam recuperáveis.

[AWS Backup](#) é um serviço totalmente gerenciado que centraliza e automatiza o backup de dados. Serviços da AWS Ele oferece suporte a vários tipos de AWS recursos e ajuda você a implementar e manter uma estratégia de backup para cargas de trabalho que usam vários AWS recursos que devem ser copiados coletivamente. AWS Backup também ajuda você a monitorar coletivamente uma operação de backup e restauração de vários AWS recursos.

AWS Backup O [Vault Lock](#) é um recurso opcional de um cofre de backup e pode fornecer segurança e controle adicionais. Quando um bloqueio está ativo no modo de Conformidade e o tempo de carência termina, a configuração do cofre não pode ser alterada ou excluída por um usuário, proprietário da conta ou dos dados, ou. AWS Cada cofre pode ter um bloqueio de cofre em vigor. Isso fornece a configuração Write Once, Read-Many (WORM) e a aplicação de períodos de retenção.

Se você seguir a orientação de configuração atual, AWS Backup pode fornecer 99,999999999% de durabilidade anual, também conhecida como 11 nines. Ele usa a infraestrutura AWS global para replicar seus backups em várias zonas de disponibilidade. Para ter mais informações, consulte [Resiliência no AWS Backup](#).

AWS Backup ajuda você a automatizar a recuperação e o teste de dados de backup para verificar a integridade e os processos de backup.

Melhores práticas relacionadas no AWS Well-Architected Framework

- [SEC09-BP01 Implemente o gerenciamento seguro de chaves e certificados](#)
- [SEC09-BP02 Impor a criptografia em trânsito](#)
- [SEC09-BP03 Autenticar as comunicações de rede](#)

Implementando este tema

Automatize o backup e a recuperação de dados

- [Implemente o backup de dados em AWS](#)
- [Automatize o backup de dados em grande escala](#) (postagem no AWS blog)
- [Automatize a validação da recuperação de dados com AWS Backup](#) (postagem AWS no blog)

Implemente a governança em seus AWS Backup resultados

- [As 10 melhores práticas de segurança para proteger backups em AWS](#) (postagem AWS do blog)
- [Use o AWS Backup Vault Lock para melhorar a segurança de seus cofres de backup](#)
- [Use o AWS Backup Audit Manager para auditar a conformidade de suas AWS Backup políticas](#)

Monitorando este tema

Implemente as seguintes AWS Config regras

- RDS_IN_BACKUP_PLAN
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- REDSHIFT_BACKUP_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- DB_INSTANCE_BACKUP_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tema 7: Centralizar o registro e o monitoramento

Oito estratégias essenciais abordadas

Controle de aplicativos, aplicativos de patches, restrição de privilégios administrativos, autenticação multifatorial

AWS fornece ferramentas e recursos que permitem que você veja o que está acontecendo em seu AWS ambiente. Isso inclui:

- [AWS CloudTrail](#) ajuda você a monitorar suas AWS implantações criando uma trilha histórica de chamadas de AWS API para sua conta, incluindo chamadas de API feitas por meio das ferramentas de linha de comando AWS Management Console AWS SDKs, e. Para serviços compatíveis CloudTrail, você também pode identificar quais usuários e contas chamaram a API do serviço, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram.
- CloudWatchA [Amazon](#) ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- O [Amazon CloudWatch Logs](#) ajuda você a centralizar os registros de todos os seus sistemas e aplicativos, Serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- GuardDutyA [Amazon](#) é um serviço contínuo de monitoramento de segurança que analisa e processa registros para identificar atividades inesperadas e potencialmente não autorizadas em seu AWS ambiente. GuardDuty se integra à Amazon EventBridge para iniciar uma resposta automática ou notificar uma pessoa.
- [AWS Security Hub](#) fornece uma visão abrangente do seu estado de segurança em AWS. Também ajuda você a verificar seu AWS ambiente de acordo com os padrões e as melhores práticas do setor de segurança.

Essas ferramentas e recursos foram projetados para aumentar a visibilidade e ajudá-lo a resolver problemas antes que eles afetem negativamente seu ambiente. Isso ajuda você a melhorar a postura de segurança da sua organização na nuvem e reduz o perfil de risco do seu ambiente.

Melhores práticas relacionadas no AWS Well-Architected Framework

- [SEC04-BP01 Configurar o registro em log de serviços e aplicações](#)
- [SEC04-BP02 Capture registros, descobertas e métricas em locais padronizados](#)

Implementando este tema

Habilitar registro em log

- [Use o CloudWatch agente para publicar registros em nível de sistema no Logs CloudWatch](#)
- [Configure alertas para GuardDuty descobertas](#)
- [Crie uma trilha organizacional em CloudTrail](#)

Implemente as melhores práticas de segurança de registro

- [Implemente as melhores práticas de CloudTrail segurança](#)
- [Use SCPs para impedir que os usuários desativem os serviços de segurança](#) (postagem AWS no blog)
- [Criptografe dados de registro no CloudWatch Logs usando AWS Key Management Service](#)

Centralize os registros

- [Receba CloudTrail registros de várias contas](#)
- [Enviar registros para uma conta de arquivamento de registros](#)
- [Centralize CloudWatch os registros em uma conta para auditoria e análise](#) (AWS postagem no blog)
- [Centralize o gerenciamento do Amazon Inspector](#)
- [Crie um agregador para toda a organização em AWS Config](#) (postagem do blog)AWS
- [Centralize o gerenciamento do Security Hub](#)
- [Centralize o gerenciamento de GuardDuty](#)
- [Considere usar o Amazon Security Lake](#)

Monitorando este tema

Implementar mecanismos

- Estabeleça um mecanismo para revisar as descobertas do registro
- Estabeleça um mecanismo para analisar as descobertas do Security Hub
- Estabeleça um mecanismo para responder às GuardDuty descobertas

Implemente as seguintes AWS Config regras

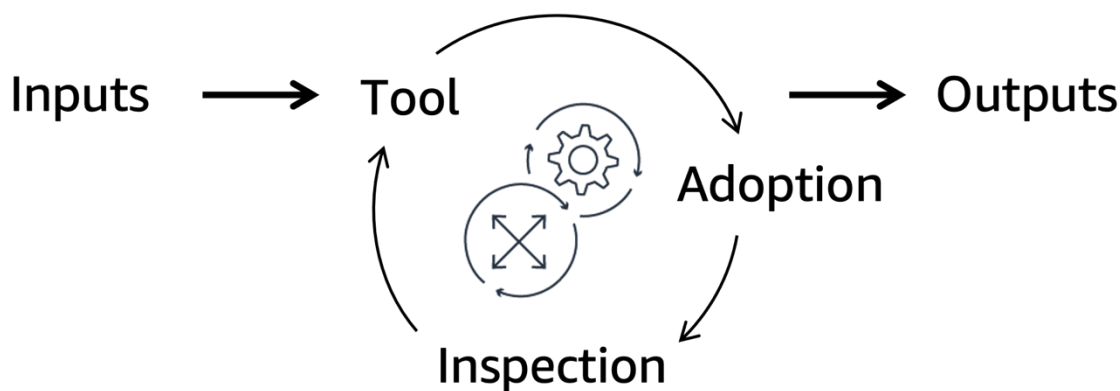
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- GUARDDUTY_ENABLED_CENTRALIZED
- SECURITYHUB_ENABLED
- ACCOUNT_PART_OF_ORGANIZATIONS

Tema 8: Implementar mecanismos para processos manuais

- 📘 Oito estratégias essenciais abordadas
 - Controle de aplicativos, aplicativos de patch

Na Amazon, temos um ditado: [Boas intenções não funcionam — mecanismos funcionam](#) (postagem AWS no blog). Isso significa que você deve substituir os melhores esforços por processos e ferramentas automatizados, repetíveis e escaláveis para alcançar os resultados desejados.

Conforme mostrado no diagrama a seguir, um mecanismo é um processo completo em que você cria uma ferramenta, impulsiona a adoção da ferramenta e, em seguida, inspeciona os resultados para fazer os ajustes. É um ciclo que se reforça e se aprimora à medida que opera. Ele usa entradas controláveis e as transforma em saídas contínuas para enfrentar um desafio comercial recorrente. Para obter mais informações, consulte [Construindo mecanismos](#) no AWS Well-Architected Framework.



Melhores práticas relacionadas no AWS Well-Architected Framework

- [OPS02-BP01 Recursos com proprietários identificados](#)
- [OPS02-BP02 Processos e procedimentos com proprietários identificados](#)
- [OPS02-BP03 Atividades de operações com proprietários identificados responsáveis pela performance](#)

- [OPS02-BP04 Mecanismos disponíveis para gerenciar responsabilidades e a relação de propriedade](#)
- [OPS03-BP01 Fornecer patrocínio executivo](#)
- [OPS03-BP03 Incentivo à escalação](#)

Implementando este tema

- Estabeleça mecanismos para analisar e resolver as lacunas de conformidade
- Estabeleça mecanismos para atualizar as políticas de segurança
- Remova os aplicativos que não são suportados e adicione-os à lista de negação de AWS Config regras
- Valide as políticas de acesso com AWS Identity and Access Management Access Analyzer
- Ative o Amazon Inspector, que mantém automaticamente os registros de vulnerabilidade up-to-date
- No mínimo, revise os conjuntos de regras de controle de aplicativos anualmente
- Considere a implementação de automação, como [AWS Config regras](#), para reduzir a carga dos processos manuais
- Considere usar o [AWS Systems Manager Inventory](#) para obter visibilidade sobre quais instâncias estão executando o software exigido pela sua política de software

Monitorando este tema

- Estabeleça uma supervisão para patrocinadores executivos que possam acompanhar o progresso em direção às metas, incluindo conformidade, inspeção de lacunas e avaliação de mecanismos.

Estudo de caso indicativo para atingir a maturidade do Essential Eight em AWS

Este capítulo apresenta um estudo de caso indicativo para uma agência governamental que visa a maturidade do Essential Eight em AWS.

Seções neste capítulo:

- [Visão geral do cenário e da arquitetura](#)
- [Exemplo de carga de trabalho: data lake sem servidor](#)
- [Exemplo de carga de trabalho: serviço web em contêineres](#)
- [Exemplo de carga de trabalho: software COTS na Amazon EC2](#)

Visão geral do cenário e da arquitetura

A agência governamental tem três cargas de trabalho no Nuvem AWS:

- Um [data lake sem servidor que usa](#) o Amazon Simple Storage Service (Amazon S3) para armazenamento AWS Lambda e operações de extração, transformação e carregamento (ETL)
- Um [serviço web em contêineres](#) que é executado no Amazon Elastic Container Service (Amazon ECS) e usa um banco de dados no Amazon Relational Database Service (Amazon RDS)
- Um [software comercial off-the-shelf \(COTS\)](#) executado na Amazon EC2

Uma equipe de nuvem fornece uma plataforma centralizada para a organização, executando os principais serviços para o AWS meio ambiente. Uma equipe de nuvem fornece serviços essenciais para o AWS meio ambiente. Cada carga de trabalho pertence a uma equipe de aplicativos distinta, também conhecida como equipe de desenvolvedores ou equipe de entrega.

Arquitetura principal

A equipe de nuvem já estabeleceu os seguintes recursos no Nuvem AWS:

- A federação de identidade está AWS IAM Identity Center vinculada a seus Microsoft Insira a instância ID (anteriormente Azure Active Directory). A federação impõe o MFA, a expiração automática das contas de usuário e o uso de credenciais AWS Identity and Access Management de curta duração por meio de funções (IAM).

- Um pipeline de AMI centralizado é usado para corrigir OSs e implantar o núcleo de aplicativos com o EC2 Image Builder.
- O Amazon Inspector está habilitado para identificar vulnerabilidades, e todas as descobertas de segurança são enviadas à Amazon GuardDuty para gerenciamento centralizado.
- Mecanismos estabelecidos são usados para atualizar as regras de controle de aplicativos, responder a eventos de segurança cibernética e analisar as lacunas de conformidade.
- AWS CloudTrail é usado para registro e monitoramento.
- Eventos de segurança, como login do usuário root, iniciam alertas.
- SCPs e as políticas de VPC endpoint estabelecem perímetros de dados para seus ambientes. AWS
- SCPs impedir que as equipes de aplicativos desativem serviços de segurança e registro, como CloudTrail e. AWS Config
- AWS Config as descobertas são agregadas de toda a AWS organização em uma única Conta da AWS para fins de segurança.
- O [pacote de conformidade AWS Config ACSC Essential 8 está disponível](#) Contas da AWS em toda a sua organização.

Exemplo de carga de trabalho: data lake sem servidor

Essa carga de trabalho é um exemplo de. [Tema 1: Usar serviços gerenciados](#)

O data lake usa o Amazon S3 para armazenamento e ETL AWS Lambda . Esses recursos são definidos em um AWS Cloud Development Kit (AWS CDK) aplicativo. As alterações no sistema são implantadas por meio AWS CodePipeline de. Esse pipeline é restrito à equipe de aplicativos. Quando a equipe do aplicativo faz uma pull request para o repositório de código, a [regra de duas pessoas é usada](#).

Para essa carga de trabalho, a equipe de aplicativos realiza as seguintes ações para abordar as estratégias Essential Eight.

Controle de aplicativos

- A equipe de aplicativos habilita a [Proteção Lambda e a digitalização GuardDuty Lambda no Amazon Inspector](#).
- A equipe de aplicação implementa mecanismos para inspecionar e [gerenciar as descobertas do Amazon Inspector](#).

Aplicativos de patch

- A equipe de aplicativos habilita o escaneamento Lambda no Amazon Inspector e configura alertas para bibliotecas obsoletas ou vulneráveis.
- A equipe de aplicativos AWS Config permite rastrear AWS recursos para descoberta de ativos.

Restringir privilégios administrativos

- Conforme descrito na [Arquitetura principal](#) seção, a equipe de aplicativos já restringe o acesso às implantações de produção por meio de uma regra de aprovação em seu pipeline de implantação.
- A equipe de aplicativos conta com as soluções centralizadas de federação de identidade e registro centralizado descritas na seção. [Arquitetura principal](#)
- A equipe do aplicativo cria uma AWS CloudTrail trilha e CloudWatch filtros da Amazon.
- A equipe do aplicativo configura alertas do Amazon Simple Notification Service (Amazon SNS) CodePipeline para implantações AWS CloudFormation e exclusões de pilhas.

Patch de sistemas operacionais

- A equipe de aplicativos habilita o escaneamento Lambda no Amazon Inspector e configura alertas para bibliotecas obsoletas ou vulneráveis.

Autenticação multifator

- A equipe de aplicativos conta com a solução centralizada de federação de identidades descrita na [Arquitetura principal](#) seção. Essa solução aplica a MFA, registra autenticações e alerta ou responde automaticamente a eventos suspeitos de MFA.

Backups regulares

- [A equipe de aplicativos armazena códigos, como AWS CDK aplicativos e funções e configurações do Lambda, em um repositório de código.](#)
- A equipe de aplicativos habilita o controle de versões e o Amazon S3 Object Lock para ajudar a evitar que objetos sejam excluídos ou modificados.
- A equipe de aplicativos confia na durabilidade integrada do Amazon S3 em vez de replicar todo o conjunto de dados em outro. Região da AWS

- A equipe de aplicativos executa uma cópia da carga de trabalho em outra Região da AWS que atenda aos requisitos de soberania de dados. Eles usam as tabelas globais do Amazon DynamoDB e a replicação [entre regiões do Amazon S3 para replicar dados automaticamente da região](#) primária para a região secundária.

Exemplo de carga de trabalho: serviço web em contêineres

Essa carga de trabalho é um exemplo de. [Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras](#)

O serviço web é executado no Amazon ECS e usa um banco de dados no Amazon RDS. A equipe do aplicativo define esses recursos em um AWS CloudFormation modelo. Os contêineres são criados com o EC2 Image Builder e armazenados no Amazon ECR. A equipe de aplicativos implanta as alterações no sistema por meio AWS CodePipeline de. Esse pipeline é restrito à equipe de aplicativos. Quando a equipe do aplicativo faz uma pull request para o repositório de código, a [regra de duas pessoas é usada](#).

Para essa carga de trabalho, a equipe de aplicativos realiza as seguintes ações para abordar as estratégias Essential Eight.

Controle de aplicativos

- A equipe do aplicativo permite a [digitalização de imagens de contêineres do Amazon ECR no Amazon Inspector](#).
- A equipe do aplicativo cria a ferramenta de segurança [File Access Policy Daemon \(fapolicyd\)](#) no pipeline do Image Builder. EC2 Para obter mais informações, consulte [Implementando o controle de aplicativos](#) no site do ACSC.
- A equipe do aplicativo configura a definição da tarefa do Amazon ECS para registrar a saída no Amazon CloudWatch Logs.
- A equipe de aplicação implementa mecanismos para inspecionar e gerenciar as descobertas do Amazon Inspector.

Aplicativos de patch

- A equipe de aplicativos permite a digitalização de imagens de contêineres do Amazon ECR no Amazon Inspector e configura alertas para bibliotecas obsoletas ou vulneráveis.

- A equipe do aplicativo automatiza suas respostas às descobertas do Amazon Inspector. Novas descobertas iniciam seu pipeline de implantação por meio de um EventBridge gatilho da Amazon e CodePipeline são o alvo.
- A equipe de aplicativos AWS Config permite rastrear AWS recursos para descoberta de ativos.

Restringir privilégios administrativos

- A equipe de aplicativos já está restringindo o acesso às implantações de produção por meio de uma regra de aprovação em seu pipeline de implantação.
- A equipe de aplicativos depende da federação de identidade da equipe de nuvem centralizada para rotação de credenciais e registro centralizado.
- A equipe do aplicativo cria uma CloudTrail trilha e CloudWatch filtra.
- A equipe do aplicativo configura alertas do Amazon SNS para CodePipeline implantações e CloudFormation exclusões de pilhas.

Patch de sistemas operacionais

- A equipe de aplicativos permite a digitalização de imagens de contêineres do Amazon ECR no Amazon Inspector e configura alertas para atualizações de patches do sistema operacional.
- A equipe de aplicação automatiza sua resposta às descobertas do Amazon Inspector. Novas descobertas iniciam seu pipeline de implantação por meio de um EventBridge gatilho e CodePipeline são o alvo.
- A equipe do aplicativo assina as notificações de eventos do Amazon RDS para ser informada sobre as atualizações. Eles tomam uma decisão baseada em riscos com o proprietário da empresa sobre se devem aplicar essas atualizações manualmente ou permitir que o Amazon RDS as aplique automaticamente.
- A equipe do aplicativo configura a instância do Amazon RDS para ser um cluster de zona de multidisponibilidade, a fim de reduzir o impacto dos eventos de manutenção.

Autenticação multifator

- A equipe de aplicativos conta com a solução centralizada de federação de identidades descrita na [Arquitetura principal](#) seção. Essa solução aplica a MFA, registra autenticações e alerta ou responde automaticamente a eventos suspeitos de MFA.

Backups regulares

- A equipe do aplicativo configura AWS Backup para automatizar o backup dos dados em seu cluster Amazon RDS.
- A equipe do aplicativo armazena CloudFormation modelos em um repositório de código.
- A equipe de aplicativos desenvolve um pipeline automatizado para [criar uma cópia de sua carga de trabalho em outra região e executar testes automatizados](#) (postagem AWS no blog). Depois que os testes automatizados são executados, o pipeline destrói a pilha. Esse pipeline é executado automaticamente uma vez por mês e valida a eficácia dos procedimentos de recuperação.

Exemplo de carga de trabalho: software COTS na Amazon EC2

Essa carga de trabalho é um exemplo de. [Tema 3: Gerenciar infraestrutura mutável com automação](#)

A carga de trabalho em execução na Amazon EC2 foi criada manualmente usando o. AWS Management Console Os desenvolvedores atualizam manualmente o sistema fazendo login nas EC2 instâncias e atualizando o software.

Para essa carga de trabalho, as equipes de nuvem e aplicativos realizam as seguintes ações para abordar as estratégias Essential Eight.

Controle de aplicativos

- A equipe de nuvem configura seu pipeline centralizado de AMI para instalar e configurar o AWS Systems Manager agente (agente SSM), o CloudWatch agente e. SELinux Eles compartilham a AMI resultante em todas as contas da organização.
- A equipe de nuvem usa AWS Config regras para confirmar que todas as [EC2 instâncias em execução são gerenciadas pelo Systems Manager](#) e têm o [SSM Agent, o CloudWatch agente e SELinux instalados](#).
- A equipe de nuvem envia a saída do Amazon CloudWatch Logs para uma solução centralizada de gerenciamento de informações e eventos de segurança (SIEM) que é executada no Amazon OpenSearch Service.
- A equipe de aplicação implementa mecanismos para inspecionar e gerenciar descobertas do AWS Config GuardDuty, e do Amazon Inspector. A equipe de nuvem implementa seus próprios mecanismos para capturar quaisquer descobertas que a equipe de aplicativos não tenha percebido. Para obter mais orientações sobre a criação de um programa de gerenciamento de

vulnerabilidades para abordar as descobertas, consulte [Criando um programa de gerenciamento de vulnerabilidades escalável em AWS](#).

Aplicativos de patch

- A equipe de aplicativos corrige instâncias com base nas descobertas do Amazon Inspector.
- A equipe de nuvem corrige a AMI básica, e a equipe de aplicativos recebe um alerta quando essa AMI é alterada.
- A equipe de aplicativos restringe o acesso direto às suas EC2 instâncias configurando [regras de grupos de segurança](#) para permitir tráfego somente nas portas exigidas pela carga de trabalho.
- A equipe de aplicativos usa o [Patch Manager](#) para corrigir instâncias em vez de fazer login em instâncias individuais.
- Para executar comandos arbitrários em grupos de EC2 instâncias, a equipe de aplicativos usa o [Run Command](#).
- Nas raras ocasiões em que a equipe de aplicativos precisa de acesso direto a uma instância, ela usa o [Gerenciador de Sessões](#). Essa abordagem de acesso usa identidades federadas e registra qualquer atividade da sessão para fins de auditoria.

Restringir privilégios administrativos

- A equipe de aplicativos configura [as regras do grupo de segurança](#) para permitir o tráfego somente nas portas exigidas pela carga de trabalho. Isso restringe o acesso direto às EC2 instâncias da Amazon e exige que os usuários acessem as EC2 instâncias por meio do Session Manager.
- A equipe de aplicativos depende da federação de identidade da equipe de nuvem centralizada para rotação de credenciais e registro centralizado.
- A equipe do aplicativo cria uma CloudTrail trilha e CloudWatch filtra.
- A equipe do aplicativo configura alertas do Amazon SNS para CodePipeline implantações e CloudFormation exclusões de pilhas.

Patch de sistemas operacionais

- A equipe de nuvem corrige a AMI básica, e a equipe de aplicativos recebe um alerta quando essa AMI é alterada. A equipe de aplicativos implanta novas instâncias usando essa AMI e, em seguida, usa o [State Manager](#), um recurso do Systems Manager, para instalar o software necessário.

- A equipe de aplicativos usa o Patch Manager para corrigir instâncias, instância de login em instâncias individuais.
- Para executar comandos arbitrários em grupos de EC2 instâncias, a equipe de aplicativos usa o Run Command.
- Nas raras ocasiões em que a equipe de aplicativos precisa de acesso direto, ela usa o Gerenciador de Sessões.

Autenticação multifator

- A equipe de aplicativos conta com a solução centralizada de federação de identidades descrita na [Arquitetura principal](#) seção. Essa solução aplica a MFA, registra autenticações e alerta ou responde automaticamente a eventos suspeitos de MFA.

Backups regulares

- A equipe de aplicativos cria um AWS Backup plano para suas EC2 instâncias e volumes do Amazon Elastic Block Store (Amazon EBS).
- A equipe de aplicativos implementa um mecanismo para realizar uma restauração de backup manualmente todos os meses.

Recursos

AWS documentação

- [AWS Arquitetura de referência de segurança \(AWS SRA\)](#)
- [AWS documentação de segurança](#)
- [Pilar de segurança do AWS Well-Architected Framework](#)

Outros AWS recursos

- [AWS Segurança na nuvem](#)
- [AWS Estrutura de adoção da nuvem](#) (perspectiva de segurança)

Recursos do Australian Cyber Security Center

- [Explicação dos oito essenciais](#)
- [Modelo essencial de oito maturidades](#)
- [Guia do processo de avaliação Essential Eight](#)

Colaboradores

Os colaboradores deste documento incluem:

- James Kingsmill, arquiteto sênior de soluções, AWS arquitetura de soluções
- Chris Harding, arquiteto sênior de soluções, arquitetura de AWS soluções
- Jess Modini, arquiteta de soluções consultivas, arquitetura de soluções AWS
- Justin Bowden, diretor de garantia de segurança, AWS garantia de segurança
- Rob Powell, arquiteto sênior de soluções, AWS arquitetura de soluções
- Tony Mihaljevic, arquiteto sênior de nuvem, serviços profissionais AWS
- Volker Rath, consultor de segurança principal da AWS Global Services Security

Apêndice: Matrizes de controles Essential Eight

As tabelas a seguir vinculam as estratégias Essential Eight à orientação de AWS implementação e às melhores práticas relevantes no AWS Well-Architected Framework. Para os controles Essential Eight que não são aplicáveis no Nuvem AWS, a tabela inclui um link para orientações adicionais do Australian Cyber Security Centre (ACSC).

Matrizes de controle:

- [Controle de aplicativos](#)
- [Aplicativos de patch](#)
- [Configurar Microsoft Office configurações de macro](#)
- [Fortalecimento de aplicativos do usuário](#)
- [Restringir privilégios administrativos](#)
- [Patch de sistemas operacionais](#)
- [Autenticação multifator](#)
- [Backups regulares](#)

Controle de aplicativos

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
O controle de aplicativos é implementado em estações de trabalho e servidores para restringir a execução de executáveis, bibliotecas de software, scripts, instaladores, HTML compilado, aplicativos HTML, miniaplicativos e	Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras : Implemente a AMI e os pipelines de criação de contêineres	Use o EC2 Image Builder e incorpore: • AWS Systems Manager Agente (agente SSM) • Ferramentas de segurança para controle de aplicativos, como Security Enhanced Linux (SELinux) (GitHub),	SEC06-BP02 Provisione computação a partir de imagens reforçadas

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
drivers do painel de controle a um conjunto aprovado pela organização.		File Access Policy Daemon (fapolicyd) () ou OpenSCAP GitHub CloudWatch Agente da Amazon Compartilhe AMIs com toda a organização Certifique-se de que as equipes de aplicativos estejam referenciando as últimas AMIs Use seu pipeline de AMI para gerenciamento de patches	
MicrosoftAs 'regras de bloqueio recomendadas' da estão implementadas.	Consulte Implementação do controle de aplicativos (site do ACSC)	Não aplicável	Não aplicável
MicrosoftAs “regras recomendadas de bloqueio de drivers” da foram implementadas.			

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Os conjuntos de regras de controle de aplicativos são validados anualmente e ou com mais frequência.	Tema 8: Implementar mecanismos para processos manuais : Implementar mecanismo para atualizar as políticas de segurança	Indisponível	SEC01-BP08 Avalie e implemente novos serviços e recursos de segurança regularmente
As execuções permitidas e bloqueadas em estações de trabalho e servidores são registradas centralmente e protegidas contra modificações e exclusões não autorizadas, monitoradas em busca de sinais de comprometimento e acionadas quando eventos de segurança cibernética são detectados.	Tema 7: Centralizar o registro e o monitoramento : Ativar registro	Use o CloudWatch agente para publicar registros em nível de sistema no Logs CloudWatch Configure alertas para GuardDuty descobertas Crie uma trilha organizacional em CloudTrail Proteja os dados armazenados no Amazon S3 usando o controle de versão e o S3 Object Lock	SEC04-BP01 Configurar o registro em log de serviços e aplicações SEC04-BP02 Capture registros, descobertas e métricas em locais padronizados

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
	Tema 7: Centralizar o registro e o monitoramento: Implemente as melhores práticas de segurança de registro	Implemente as melhores práticas de CloudTrail segurança Use SCPs para impedir que os usuários desativem os serviços de segurança (postagem AWS no blog) Criptografe dados de registro no CloudWatch Logs usando AWS Key Management Service	SEC04-BP01 Configurar o registro em log de serviços e aplicações SEC04-BP02 Capture registros, descobertas e métricas em locais padronizados

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
	Tema 7: Centralizar o registro e o monitoramento: Centralize os registros	Receba CloudTrail registros de várias contas Enviar registros para uma conta de arquivamento de registros Centralize CloudWatch os registros em uma conta para auditoria e análise (AWS postagem no blog) Centralize o gerenciamento do Amazon Inspector Crie um agregador para toda a organização em AWS Config (postagem do blog)AWS Centralize o gerenciamento do Security Hub Centralize o gerenciamento de GuardDuty	SEC04-BP02 Capture registros, descobertas e métricas em locais padronizados

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
		Considere usar o Amazon Security Lake	
	Tema 8: Implementar mecanismos para processos manuais : Implementar mecanismos para analisar e resolver as lacunas de conformidade	Considere a implementação de automação, como AWS Config regras , para reduzir a carga dos processos manuais	OPS02-BP02 Processos e procedimentos com proprietários identificados OPS02-BP03 Atividades de operações com proprietários identificados responsáveis pela performance OPS02-BP04 Mecanismos disponíveis para gerenciar responsabilidades e a relação de propriedade

Aplicativos de patch

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Um método automatizado de descoberta de ativos é usado pelo menos quinzenalmente para apoiar a	Tema 1: Usar serviços gerenciados : Verifique se há vulnerabilidades	Habilite o Amazon Inspector em todas as contas da sua organização	SEC06-BP01 Execute o gerenciamento de vulnerabilidades

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
detecção de ativos para atividades subsequentes de verificação de vulnerabilidades.	Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras: Implemente e a verificação de vulnerabilidades Tema 3: Gerenciar infraestrutura mutável com automação: Implemente a verificação de vulnerabilidades	Configure a digitalização aprimorada para repositórios do Amazon ECR usando o Amazon Inspector Crie um programa de gerenciamento de vulnerabilidades para fazer a triagem e corrigir as descobertas de segurança	SEC06-BP05 Automatize a proteção computacional

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
	Tema 7: Centralizar o registro e o monitoramento: Centralize os registros	Receba CloudTrail registros de várias contas Enviar registros para uma conta de arquivamento de registros Centralize CloudWatch os registros em uma conta para auditoria e análise (AWS postagem no blog) Centralize o gerenciamento do Amazon Inspector Crie um agregador para toda a organização em AWS Config (postagem do blog)AWS Centralize o gerenciamento do Security Hub Centralize o gerenciamento de GuardDuty Considere usar o Security Lake	SEC04-BP02 Capture registros, descobertas e métricas em locais padronizados

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Um scanner de vulnerabilidade com um banco de dados de up-to-dat e vulnerabilidades é usado para atividades de verificação de vulnerabilidades.	Tema 1: Usar serviços gerenciados: Verifique se há vulnerabilidades Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras: Implemente e a verificação de vulnerabilidades Tema 3: Gerenciar infraestrutura mutável com automação: Implemente a verificação de vulnerabilidades	Habilite o Amazon Inspector em todas as contas da sua organização Configure a digitalização aprimorada para repositórios do Amazon ECR usando o Amazon Inspector Crie um programa de gerenciamento de vulnerabilidades para fazer a triagem e corrigir as descobertas de segurança	SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP05 Automatize a proteção computacional
Um scanner de vulnerabilidade é usado pelo menos diariamente para identificar patches ou atualizações ausentes para vulnerabilidades de segurança em serviços voltados para a Internet.			

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Um scanner de vulnerabilidade é usado pelo menos semanalmente para identificar patches ou atualizações ausentes para vulnerabilidades de segurança em suítes de produtividade de escritório, navegadores da Web e suas extensões, clientes de e-mail, software de PDF e produtos de segurança.	Veja o exemplo técnico: aplicativos de patch (site do ACSC)	Não aplicável	Não aplicável

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Um scanner de vulnerabilidade é usado pelo menos quinzenalmente para identificar patches ou atualizações ausentes para vulnerabilidades de segurança em outros aplicativos.	Tema 1: Usar serviços gerenciados: Verifique se há vulnerabilidades Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras: Implemente e a verificação de vulnerabilidades Tema 3: Gerenciar infraestrutura mutável com automação: Implemente a verificação de vulnerabilidades	Habilite o Amazon Inspector em todas as contas da sua organização Configure a digitalização aprimorada para repositórios do Amazon ECR usando o Amazon Inspector Crie um programa de gerenciamento de vulnerabilidades para fazer a triagem e corrigir as descobertas de segurança	SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP05 Automatize a proteção computacional

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Patches, atualizações ou mitigações do fornecedor para vulnerabilidades de segurança em serviços voltados para a Internet são aplicados dentro de duas semanas após o lançamento, ou dentro de 48 horas se houver uma exploração.	Tema 1: Usar serviços gerenciados: Verifique se há vulnerabilidades Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras: Implemente e a verificação de vulnerabilidades Tema 3: Gerenciar infraestrutura mutável com automação: Implemente a verificação de vulnerabilidades	Habilite o Amazon Inspector em todas as contas da sua organização Configure a digitalização aprimorada para repositórios do Amazon ECR usando o Amazon Inspector Crie um programa de gerenciamento de vulnerabilidades para fazer a triagem e corrigir as descobertas de segurança	SEC06-BP01 Execute o gerenciamento de vulnerabilidades
	Tema 3: Gerenciar infraestrutura mutável com automação: Automatize a aplicação de patches	Ative o Patch Manager em todas as contas AWS da sua organização	SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP05 Automatize a proteção computacional

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Patches, atualizações ou mitigações de fornecedores para vulnerabilidades de segurança em suítes de produtividade de escritório, navegadores da Web e suas extensões, clientes de e-mail, software de PDF e produtos de segurança são aplicados dentro de duas semanas após o lançamento ou dentro de 48 horas se houver uma exploração.	Veja o exemplo técnico: aplicativos de patch (site do ACSC)	Não aplicável	Não aplicável

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Patches, atualizações ou mitigações do fornecedor para vulnerabilidades de segurança em outros aplicativos são aplicados dentro de um mês após o lançamento.	Tema 1: Usar serviços gerenciados: Verifique se há vulnerabilidades Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras: Implemente e a verificação de vulnerabilidades Tema 3: Gerenciar infraestrutura mutável com automação: Implemente a verificação de vulnerabilidades	Habilite o Amazon Inspector em todas as contas da sua organização Configure a digitalização aprimorada para repositórios do Amazon ECR usando o Amazon Inspector Crie um programa de gerenciamento de vulnerabilidades para fazer a triagem e corrigir as descobertas de segurança	SEC06-BP01 Execute o gerenciamento de vulnerabilidades
	Tema 3: Gerenciar infraestrutura mutável com automação: Automatize a aplicação de patches	Ative o Patch Manager em todas as contas AWS da sua organização	SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP05 Automatize a proteção computacional

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Os aplicativos que não são mais suportados pelos fornecedores são removidos.	Tema 8: Implementar mecanismos para processos manuais : Implementar mecanismos para analisar e resolver as lacunas de conformidade	Considere usar o AWS Systems Manager Inventory para obter visibilidade sobre quais instâncias estão executando o software exigido pela sua política de software	SEC06-BP02 Provisione computação a partir de imagens reforçadas

Configurar Microsoft Office configurações de macro

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Microsoft Office as macros são desativadas para usuários que não têm uma exigência comercial comprovada.	Veja o exemplo técnico: Definir configurações de macro (site do ACSC)	Não aplicável	Não aplicável
Somente Microsoft Office macros executadas em um ambiente de área restrita, em um local confiável ou assinadas digitalmente por um editor confiável podem ser executadas.			

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Somente usuários privilegiados responsáveis por validar isso Microsoft Office as macros estão livres de códigos maliciosos e podem gravar e modificar conteúdo em Locais Confiáveis.			
Microsoft Office macros assinadas digitalmente por um editor não confiável não podem ser habilitadas por meio da Barra de Mensagens ou do Backstage View.			
Microsoft OfficeA lista de editores confiáveis da é validada anualmente ou com mais frequência.			
Microsoft Office macros em arquivos provenientes da Internet são bloqueadas.			

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Microsoft Office a verificação antivírus de macros está ativada.			
Microsoft Office as macros estão impedidas de criar Win32 Chamadas de API.			
Microsoft Office as configurações de segurança de macro não podem ser alteradas pelos usuários.			
Permitido e bloqueado Microsoft Office as execuções de macros são registradas centralmente e protegidas contra modificações e exclusões não autorizadas, monitoradas em busca de sinais de comprometimento e acionadas quando eventos de segurança cibernética são detectados.			

Fortalecimento de aplicativos do usuário

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Os navegadores da Web não processam Java da internet.	Veja o exemplo técnico: fortalecimento de aplicativos do usuário (site do ACSC)	Não aplicável	Não aplicável
Os navegadores da Web não processam anúncios da Internet.			
Internet Explorer 11 está desativado ou removido.			
Microsoft Office está impedido de criar processos secundários.			
Microsoft Office está impedido de criar conteúdo executável.			
Microsoft Office está impedido de injetar código em outros processos.			
Microsoft Office está configurado para impedir a ativação de pacotes OLE.			
O software PDF está impedido de criar			

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
processos secundários.			
Guia de proteção do ACSC ou do fornecedor para navegadores da web, Microsoft Office e o software PDF é implementado.			
Navegador da Web, Microsoft Office e as configurações de segurança do software PDF não podem ser alteradas pelos usuários.			
.NET Framework 3.5 (inclui .NET 2.0 e 3.0) está desativado ou removido.			
Windows PowerShell 2.0 está desativado ou removido.			
PowerShell está configurado para usar o Modo de Linguagem Restrita.			

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Bloqueado PowerShell as execuções de scripts são registradas centralmente e protegidas contra modificações e exclusões não autorizadas, monitoradas em busca de sinais de comprometimento e acionadas quando eventos de segurança cibernética são detectados.			

Restringir privilégios administrativos

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
As solicitações de acesso privilegiado a sistemas e aplicativos são validadas quando solicitadas pela primeira vez.	Tema 4: Gerenciar identidades: Implementar federação de identidades	Exija que os usuários humanos se federem com um provedor de identidade para acessar AWS usando credenciais temporárias	SEC02-BP04 Confiar em um provedor de identidades centralizado SEC03-BP01 Definir requisitos de acesso
O acesso privilegiado a sistemas e aplicativos é automaticamente desativado após 12	Tema 4: Gerenciar identidades: Implementar	Exija que os usuários humanos se federem com um provedor de identidade para	SEC02-BP04 Confiar em um provedor de identidades centralizado

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
meses, a menos que seja revalidado.	federação de identidades	acessar AWS usando credenciais temporárias	
	Tema 4: Gerenciar identidades : Alterne as credenciais	Exija que as cargas de trabalho usem funções do IAM para acessar AWS Automatize a exclusão de funções do IAM não utilizadas Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo AWS Summit ANZ 2023: Sua jornada para credenciais temporárias na nuvem (YouTube vídeo)	SEC02-BP05 Auditar e fazer a rotação das credenciais periodicamente

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
O acesso privilegiado a sistemas e aplicativos é automaticamente desativado após 45 dias de inatividade.	Tema 4: Gerenciar identidades: Implementar federação de identidades Tema 4: Gerenciar identidades: Alterne as credenciais	Exija que os usuários humanos se federem com um provedor de identidade para acessar AWS usando credenciais temporárias Exija que as cargas de trabalho usem funções do IAM para acessar AWS Automatize a exclusão de funções do IAM não utilizadas Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo AWS Summit ANZ 2023: Sua jornada para credenciais temporárias na nuvem (YouTube vídeo)	SEC02-BP04 Confiar em um provedor de identidades centralizado SEC02-BP05 Auditar e fazer a rotação das credenciais periodicamente

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
O acesso privilegiado a sistemas e aplicativos é limitado apenas ao que é necessário para que usuários e serviços realizem suas tarefas.	Tema 4: Gerenciar identidades : aplique permissões de privilégio mínimo	Proteja suas credenciais de usuário root e não as use para tarefas diárias Use o IAM Access Analyzer para gerar políticas de privilégios mínimos com base na atividade de acesso Verifique o acesso público e entre contas aos recursos com o IAM Access Analyzer Use o IAM Access Analyzer para validar suas políticas do IAM para obter permissões seguras e funcionais Estabeleça barreiras de permissões em várias contas Use limites de permissões para definir o máximo de permissões que uma política baseada em identidade pode conceder	SEC01-BP02 Usuário raiz e propriedades da conta segura SEC03-BP02 Conceder acesso de privilégio mínimo

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
		Use condições nas políticas do IAM para restringir ainda mais o acesso Revise e remova regularmente usuários, funções, permissões, políticas e credenciais não utilizados Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos Use o recurso de conjuntos de permissões no IAM Identity Center	
Contas privilegiadas são impedidas de acessar a Internet, e-mail e serviços da web.	Veja o exemplo técnico: Restringir privilégios administrativos (site do ACSC)	Considere implementar um SCP que impeça que qualquer VPC que ainda não tenha acesso à Internet o obtenha	Não aplicável

Controle Essencial Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Usuários privilegiados usam ambientes operacionais privilegiados e não privilegiados separados. Ambientes operacionais privilegiados não são virtualizados em ambientes operacionais sem privilégios. Contas sem privilégios não podem fazer login em ambientes operacionais privilegiados. Contas privilegiadas (excluindo contas de administrador local) não podem fazer login em ambientes operacionais sem privilégios.	Tema 5: Estabelecer um perímetro de dados	Estabeleça um perímetro de dados. Considere implementar perímetros de dados entre ambientes de diferentes classificações de dados, como OFFICIAL : SENSITIVE ou PROTECTED , ou diferentes níveis de risco, como desenvolvimento, teste ou produção.	SEC06-BP03 Reduzir o gerenciamento manual e o acesso interativo

Controle Essencial Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Just-in-time a administração é usada para administrar sistemas e aplicativos.	Tema 4: Gerenciar identidades : Implementar federação de identidades	Exija que os usuários humanos se federem com um provedor de identidade para acessar AWS usando credenciais temporárias Implemente acesso elevado temporário aos seus AWS ambientes (postagem AWS no blog)	SEC02-BP04 Confiar em um provedor de identidades centralizado
As atividades administrativas são conduzidas por meio de servidores de salto.	Tema 1: Usar serviços gerenciados Tema 3: Gerenciar infraestrutura mutável com automação : Use automação em vez de processos manuais	Use o Gerenciador de Sessões ou Execute o Comando em vez do acesso direto por SSH ou RDP	SEC01-BP05 Reduza o escopo do gerenciamento de segurança SEC06-BP03 Reduzir o gerenciamento manual e o acesso interativo
As credenciais para contas de administrador e contas de serviço locais são exclusivas, imprevisíveis e gerenciadas.	Veja o exemplo técnico: Restringir privilégios administrativos (site do ACSC)	Não aplicável	Não aplicável

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Windows Defender Credential Guard and Windows Defender Remote Credential Guard estão habilitados.			

Controle Essencial Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
O uso do acesso privilegiado é registrado centralmente e protegido contra modificações e exclusões não autorizadas, monitorado em busca de sinais de comprometimento e acionado quando eventos de segurança cibernética são detectados.	Tema 7: Centralizar o registro e o monitoramento: Ativar registro Tema 7: Centralizar o registro e o monitoramento: Centralize os registros	Use o CloudWatch Agente para publicar registros no nível do sistema operacional no Logs CloudWatch Habilite CloudTrail para sua organização Centralize o CloudWatch os registros em uma conta para auditoria e análise (AWS postagem no blog) Centralize o gerenciamento do Amazon Inspector Centralize o gerenciamento do Security Hub Crie um agregador para toda a organização em AWS Config (postagem do blog)AWS Centralize o gerenciamento de GuardDuty Considere usar o Amazon Security Lake	SEC04-BP01 Configurar o registro em log de serviços e aplicações SEC04-BP02 Capture registros, descobertas e métricas em locais padronizados
As alterações em contas e grupos privilegiados são registradas centralmente e protegidas contra modificações e exclusões não autorizadas, monitoradas em busca de sinais de comprometimento e acionadas quando eventos de segurança cibernética são detectados.			

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
		Receba CloudTrail registros de várias contas Enviar registros para uma conta de arquivamento de registros	

Patch de sistemas operacionais

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Patches, atualizações ou mitigações do fornecedor para vulnerabilidades de segurança em sistemas operacionais de serviços voltados para a Internet são aplicados dentro de duas semanas após o lançamento, ou dentro de 48 horas se houver uma exploração.	Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras : Implemente a AMI e os pipelines de criação de contêineres	Use o EC2 Image Builder e incorpore: AWS Systems Manager Agente (agente SSM) Ferramentas de segurança para controle de aplicativos, como Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) () ou OpenSCAP GitHub CloudWatch Agente da Amazon	SEC01-BP05 Reduza o escopo do gerenciamento de segurança SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP03 Reduzir o gerenciamento manual e o acesso interativo

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
		Compartilhe AMIs com toda a organização Certifique-se de que as equipes de aplicativos estejam referenciando as últimas AMIs Use seu pipeline de AMI para gerenciamento de patches	
	Tema 1: Usar serviços gerenciados: Habilitar a aplicação de patches Tema 3: Gerenciar infraestrutura mutável com automação : Automatize a aplicação de patches	Ative o Patch Manager em todas as contas AWS da sua organização	SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP05 Automatize a proteção computacional

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Patches, atualizações ou mitigações do fornecedor para vulnerabilidades de segurança em sistemas operacionais de estações de trabalho, servidores e dispositivos de rede são aplicados dentro de duas semanas após o lançamento, ou dentro de 48 horas se houver uma exploração.	Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras : Implemente a AMI e os pipelines de criação de contêineres	Use o EC2 Image Builder e incorpore: • AWS Systems Manager Agente (agente SSM) • Ferramentas de segurança para controle de aplicativos, como Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) () ou OpenSCAP GitHub • CloudWatch Agente da Amazon Compartilhe AMIs com toda a organização Certifique-se de que as equipes de aplicativos estejam referenciando as últimas AMIs Use seu pipeline de AMI para gerenciamento de patches	SEC01-BP05 Reduza o escopo do gerenciamento de segurança SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP02 Provisione computação a partir de imagens reforçadas

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
	Tema 1: Usar serviços gerenciados: Habilitar a aplicação de patches Tema 3: Gerenciar infraestrutura mutável com automação : Automatize a aplicação de patches	Ative o Patch Manager em todas as contas AWS da sua organização	SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP05 Automatize a proteção computacional

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Um scanner de vulnerabilidade é usado pelo menos diariamente para identificar patches ou atualizações ausentes para vulnerabilidades de segurança em sistemas operacionais de serviços voltados para a Internet.	Tema 1: Usar serviços gerenciados: Verifique se há vulnerabilidades Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras: Implemente e a verificação de vulnerabilidades	Habilite o Amazon Inspector em todas as contas da sua organização Configure a digitalização aprimorada para repositórios do Amazon ECR usando o Amazon Inspector Crie um programa de gerenciamento de vulnerabilidades para fazer a triagem e corrigir as descobertas de segurança	SEC01-BP05 Reduza o escopo do gerenciamento de segurança SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP02 Provisione computação a partir de imagens reforçadas
Um scanner de vulnerabilidade é usado pelo menos semanalmente para identificar patches ou atualizações ausentes para vulnerabilidades de segurança em sistemas operacionais de estações de trabalho, servidores e dispositivos de rede.	Tema 3: Gerenciar infraestrutura mutável com automação: Implemente a verificação de vulnerabilidades		

Controle Essencial Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
A versão mais recente, ou a versão anterior, dos sistemas operacionais é usada para estações de trabalho, servidores e dispositivos de rede. Os sistemas operacionais que não são mais suportados pelos fornecedores são substituídos.	Tema 2: Gerenciar infraestrutura imutável por meio de tubulações seguras: Implemente e a verificação de vulnerabilidades	Use o EC2 Image Builder e incorpore: • AWS Systems Manager Agente (agente SSM) • Ferramentas de segurança para controle de aplicativos, como Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) () ou OpenSCAP GitHub • CloudWatch Agente da Amazon Compartilhe AMIs com toda a organização Certifique-se de que as equipes de aplicativos estejam referenciando as últimas AMIs Use seu pipeline de AMI para gerenciamento de patches	SEC01-BP05 Reduza o escopo do gerenciamento de segurança SEC06-BP01 Execute o gerenciamento de vulnerabilidades SEC06-BP02 Provisione computação a partir de imagens reforçadas

Autenticação multifator

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
A autenticação multifatorial é usada pelos usuários de uma organização se eles se autenticarem nos serviços voltados para a Internet da organização.	Tema 4: Gerenciar identidades: Implementar federação de identidades	Exija que os usuários humanos se federem com um provedor de identidade para acessar AWS usando credenciais temporárias Implemente acesso elevado temporário aos seus AWS ambientes	SEC02-BP04 Confiar em um provedor de identidades centralizado
	Tema 4: Gerenciar identidades: Imponha o MFA	Exigir MFA para o usuário raiz Exigir MFA por meio de AWS IAM Identity Center Considere exigir a MFA para ações de API específicas do serviço	SEC02-BP01 Use mecanismos de login robustos
A autenticação multifatorial é usada pelos usuários de uma organização se eles se autenticam em serviços terceirizados voltados para a Internet	Consulte Implementação da autenticação multifatorial (site do ACSC)	Não aplicável	Não aplicável

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
que processam , armazenam ou comunicam os dados confidenciais de sua organização.			
A autenticação multifatorial (quando disponível) é usada pelos usuários de uma organização se eles se autenticarem em serviços terceirizados voltados para a Internet que processam , armazenam ou comunicam os dados não confidenciais de sua organização.			
A autenticação multifator é habilitada por padrão para usuários não organizacionais (mas os usuários podem optar por não participar) se eles se autenticarem nos serviços de Internet de uma organização.			

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
A autenticação multifatorial é usada para autenticar usuários privilegiados dos sistemas.	Tema 4: Gerenciar identidades : Implementar federação de identidades	Exija que os usuários humanos se federem com um provedor de identidade para acessar AWS usando credenciais temporárias Implemente acesso elevado temporário aos seus AWS ambientes	SEC02-BP04 Confiar em um provedor de identidades centralizado
	Tema 4: Gerenciar identidades : Imponha o MFA	Exigir MFA para o usuário raiz Exigir MFA por meio do IAM Identity Center Considere exigir a MFA para ações de API específicas do serviço	SEC02-BP01 Use mecanismos de login robustos
A autenticação multifatorial é usada para autenticar usuários que acessam repositórios de dados importantes.	Tema 4: Gerenciar identidades : Imponha o MFA	Considere exigir a MFA para ações de API específicas do serviço	SEC02-BP01 Use mecanismos de login robustos

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
A autenticação multifatorial é resistente à falsificação de identidade e por verificadores e usa: algo que os usuários têm e algo que os usuários sabem, ou algo que os usuários têm que está desbloqueado por algo que os usuários conhecem ou são.	Consulte Implementação da autenticação multifatorial (site do ACSC)	Não aplicável	Não aplicável

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
As autenticações multifatoriais bem-sucedidas e malsucedidas são registradas centralmente e protegidas contra modificações e exclusões não autorizadas, monitoradas em busca de sinais de comprometimento e acionadas quando eventos de segurança cibernética são detectados.	Tema 7: Centralizar o registro e o monitoramento: Ativar registro Tema 7: Centralizar o registro e o monitoramento: Centralize os registros	Centralize CloudWatch os registros em uma conta para auditoria e análise (AWS postagem no blog) Centralize o gerenciamento do Amazon Inspector Centralize o gerenciamento do Security Hub Crie um agregador para toda a organização em AWS Config (postagem do blog)AWS Centralize o gerenciamento de GuardDuty Considere usar o Security Lake Receba CloudTrail registros de várias contas Enviar registros para uma conta de arquivamento de registros	SEC04-BP01 Configurar o registro em log de serviços e aplicações SEC04-BP02 Capture registros, descobertas e métricas em locais padronizados

Backups regulares

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
Os backups de dados, software e configurações importantes são realizados e mantidos de forma coordenada e resiliente, de acordo com os requisitos de continuidade dos negócios.	Tema 6: Automatizar backups : Automatiz e o backup e a recuperação de dados	Implemente o backup de dados em AWS Automatize o backup de dados em grande escala (postagem no AWS blog)	REL09-BP01 Identificar e fazer backup de todos os dados que precisam de backup ou reproduzir os dados das fontes REL09-BP02 Proteger e criptografar backups REL09-BP03 Fazer backup de dados automaticamente
A restauração de sistemas, software e dados importantes dos backups é testada de forma coordenada como parte dos exercícios de recuperação de desastres.	Tema 6: Automatizar backups : Automatiz e o backup e a recuperação de dados Tema 6: Automatizar backups : Implement e a governança em seus AWS Backup resultados	Automatize a validação da recuperação de dados com AWS Backup (postagem AWS no blog) Use o AWS Backup Audit Manager para auditar a conformidade de suas AWS Backup políticas	REL09-BP04 Realizar a recuperação periódica dos dados para verificar a integridade e os processos de backup
Contas sem privilégios e contas privilegiadas (excluindo administradores de	Tema 6: Automatizar backups : Implement e a governança em seus AWS Backup resultados	As 10 melhores práticas de segurança para proteger backups em AWS	SEC08-BP04 Aplicar controle de acesso

Controle Essential Eight	Orientação para implementação	AWS recursos	AWS Orientação do Well-Architected
backups) não podem acessar backups. Contas sem privilégios e contas privilegiadas (excluindo contas de backup) são impedidas de modificar ou excluir backups.		(postagem AWS do blog) Use o AWS Backup Vault Lock para melhorar a segurança de seus cofres de backup Use o AWS Backup Audit Manager para auditar a conformidade de suas AWS Backup políticas	

Avisos

Os clientes são responsáveis por fazer uma avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa ofertas e práticas atuais de AWS produtos, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia de suas afiliadas, AWS fornecedores ou licenciadores. AWS os produtos ou serviços são fornecidos “como estão” sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e obrigações de AWS seus clientes são controladas por AWS contratos, e este documento não faz parte nem modifica nenhum contrato entre AWS e seus clientes.

© 2023 Amazon Web Services, Inc. ou suas afiliadas. Todos os direitos reservados.

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
Atualizações de melhores práticas	Atualizamos este guia para refletir as melhores práticas mais recentes no pilar de segurança do AWS Well-Architected Framework.	6 de novembro de 2024
Publicação inicial	—	20 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 o. AWS
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um

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

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

A

ABAC

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

serviços abstratos

Veja os [serviços gerenciados](#).

ACID

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

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja 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 ou 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, 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 da CAF incluem gerenciamento de identidade e acesso, controles de detetive, segurança de infraestrutura, proteção de dados e resposta a incidentes. Para obter mais informações sobre epics na estratégia de migração da AWS, consulte o [guia de implementação do programa](#).

ERP

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 rápida

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 trancos](#) 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 (OUs). 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 HA 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

IaC

Veja a [infraestrutura como código](#).

Política baseada em identidade

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

aplicação ociosa

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

IIoT

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

infraestrutura imutável

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

VPC de entrada (admissão)

Em uma arquitetura de AWS várias contas, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de um aplicativo. A [Arquitetura de Referência de 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 etiquetas](#).

privilegio 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, vaziar informações confidenciais ou obter acesso não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Tróia, spyware e keyloggers.

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte [Migration Acceleration Program](#).

mecanismo

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

conta 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.](#)

microserviço

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 microserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos microserviços incluem agilidade, escalabilidade flexível, fácil implantação, código reutilizável e resiliência. Para obter mais informações, consulte [Integração de microserviços usando serviços sem AWS servidor.](#)

arquitetura de microserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microserviço. Esses microserviços se comunicam por meio de uma interface bem definida usando 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: rehospede 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 sistemas que leva em conta 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.