



Arquitetura de computação em nuvem segura (SCCA) ativada AWS para o Departamento de Defesa dos EUA

AWS Recomendações



AWS Recomendações: Arquitetura de computação em nuvem segura (SCCA) ativada AWS para o Departamento de Defesa dos EUA

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

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

Table of Contents

| | |
|---|----|
| Introdução | 1 |
| Público-alvo | 1 |
| Visão geral do Landing Zone Accelerator | 2 |
| Planejando sua implantação do LZA em AWS | 4 |
| Componentes e requisitos do SCCA | 5 |
| Ponto de acesso à nuvem | 7 |
| Pilha de segurança de data center virtual | 8 |
| Managed Services de data center virtual | 18 |
| Integração de serviços suplementares | 25 |
| Patches do sistema operacional. | 26 |
| Gerenciador de credenciais de nuvem confiável | 26 |
| Conclusão | 33 |
| Recursos | 34 |
| AWS documentação | 34 |
| Outros recursos | 34 |
| Histórico do documento | 35 |
| Glossário | 36 |
| # | 36 |
| A | 37 |
| B | 40 |
| C | 42 |
| D | 45 |
| E | 50 |
| F | 52 |
| G | 53 |
| H | 54 |
| I | 55 |
| L | 58 |
| M | 59 |
| O | 63 |
| P | 66 |
| Q | 68 |
| R | 69 |
| S | 72 |

| | |
|---------|------|
| T | 75 |
| U | 77 |
| V | 77 |
| W | 78 |
| Z | 79 |
| | lxxx |

Arquitetura de computação em nuvem segura (SCCA) ativada AWS para o Departamento de Defesa dos EUA

Rob Higareda e Rughved Gadgil, da Amazon Web Services (AWS)

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

O Departamento de Defesa dos EUA (DoD) segmenta as informações da nuvem em níveis de impacto (ILs). O nível de impacto está associado à sensibilidade das informações e ao risco de perder a confidencialidade, integridade ou disponibilidade dessas informações. O IL4 acomoda informações não classificadas controladas pelo DoD (CUI) e o IL5 acomoda as informações CUI do DoD e dos Sistemas de Segurança Nacional (NSS). Este guia foi desenvolvido para ajudá-lo a criar uma landing zone que ofereça suporte às informações de IL4 e IL5.

Para criar uma infraestrutura de nuvem compatível com IL4 ou IL5, você deve criar componentes específicos. A Arquitetura de Computação em Nuvem Segura (SCCA) da Defense Information Systems Agency (DISA) é uma seleção de serviços de gerenciamento e segurança em nuvem. Ele fornece uma abordagem padronizada para criar um limite de nuvem. O SCCA também inclui componentes de segurança em nível de aplicativo para informações IL4 e IL5 hospedadas na nuvem.

Este guia ajuda você a atender aos requisitos do SCCA usando o [Landing Zone Accelerator \(LZA\)](#) ativado. A solução LZA implanta um conjunto básico de recursos projetado para se alinhar às AWS melhores práticas e a várias estruturas globais de conformidade. O LZA pode ajudá-lo a criar muitos dos componentes necessários para aderir ao SCCA do DoD. Este guia também recomenda como você pode adicionar componentes adicionais para conformidade com a SCCA e estabelecer uma base segura para seus ambientes de nuvem em AWS. Embora este guia não inclua todas as situações em potencial, ele fornece orientações sobre como começar e quais Serviços da AWS podem ajudá-lo a atender aos requisitos do SCCA.

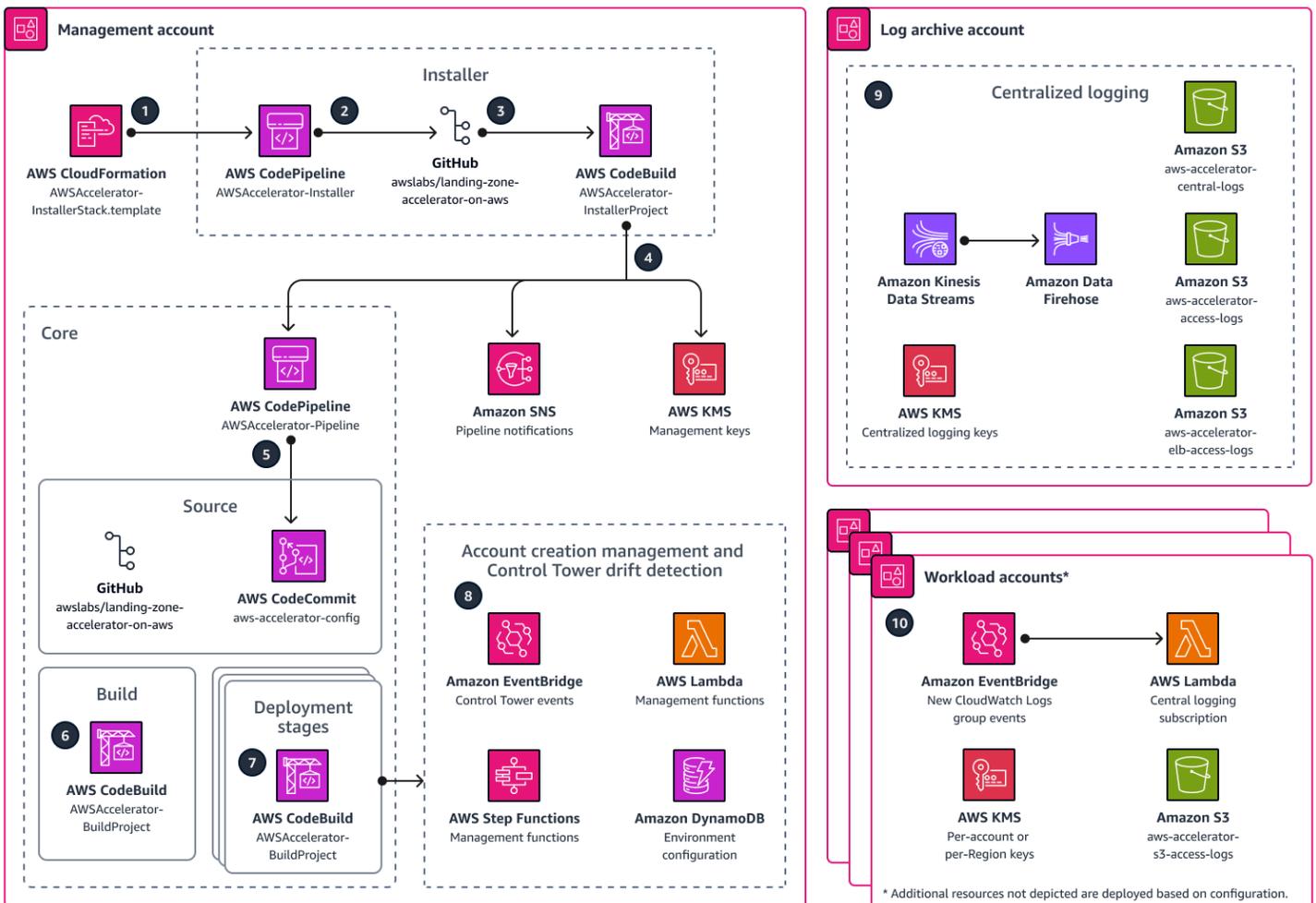
Público-alvo

Este guia é destinado a indivíduos que precisam estar em conformidade com a Arquitetura de Computação em Nuvem Segura do DoD para ajudar a proteger as informações IL4 e IL5 no. Nuvem AWS Se você ainda não fez isso, consulte o [Guia de Requisitos de Segurança de Computação em Nuvem da DISA](#) antes de ler este guia.

Visão geral do Landing Zone Accelerator

Para construir uma landing zone AWS que esteja em conformidade com a Arquitetura de Computação em Nuvem Segura (SCCA) da Agência de Sistemas de Informação de Defesa (DISA), você deve ter certos elementos para ajudá-lo a atender aos requisitos mínimos. AWS criou o [Landing Zone Accelerator \(LZA\)](#) para ajudá-lo a implantar uma zona de pouso que atenda aos requisitos necessários. Usando a solução LZA, você pode implantar o ambiente usando um conjunto de arquivos de configuração. Esses arquivos de configuração ajudam você a se concentrar na entrega de um ambiente em vez de aprender cada indivíduo AWS service (Serviço da AWS) e como implantá-lo.

A imagem a seguir mostra os serviços envolvidos na implantação do LZA. Os números indicam o fluxo de trabalho, desde a modificação dos arquivos de configuração até a configuração dos Serviços da AWS contendo a carga de trabalho.



Essa solução foi projetada para se alinhar às AWS melhores práticas e estar em conformidade com várias estruturas globais de conformidade. Quando usada em coordenação com serviços como [AWS Control Tower](#), essa solução fornece uma solução abrangente Serviços da AWS e de baixo código em mais de 35 recursos. Especificamente, essa solução ajuda você a gerenciar e governar um ambiente de várias contas criado para suportar cargas de trabalho altamente regulamentadas e requisitos complexos de conformidade. O LZA ajuda você a estabelecer a prontidão da plataforma com recursos operacionais, de segurança e de conformidade. Este guia inclui notas específicas sobre o uso dessa solução para apoiar o alinhamento com as diretrizes [federais e do Departamento de Defesa \(DoD\) dos Estados Unidos \(EUA\)](#).

AWS fornece a solução LZA como um projeto de código aberto que foi construído usando o [AWS Cloud Development Kit \(AWS CDK\)](#). Você pode instalá-lo diretamente em seu ambiente, oferecendo acesso total à solução de infraestrutura como código (IaC).

Por meio de um conjunto simplificado de arquivos de configuração, você pode:

- Configure funcionalidades adicionais, grades de proteção e serviços de segurança, como regras [AWS Config](#) e [AWS Security Hub](#)
- Gerencie sua topologia de rede básica por meio de serviços como [Amazon Virtual Private Cloud \(Amazon VPC\)](#), e [AWS Transit Gateway](#) e [AWS Network Firewall](#)
- Gere contas de carga de trabalho adicionais usando o [AWS Control Tower Account Factory](#).

Não há cobranças adicionais ou compromissos iniciais necessários para usar o Landing Zone Accelerator no. AWS. Você paga apenas pelo Serviços da AWS que ativa para configurar sua plataforma e operar suas grades de proteção. Essa solução também pode suportar AWS partições não padrão, incluindo as regiões AWS GovCloud (US), AWS Secret e AWS Top Secret.

Important

A solução LZA, por si só, não o torna compatível. Ele fornece a infraestrutura básica a partir da qual você pode integrar soluções complementares adicionais. As informações contidas no [guia de implementação do LZA](#) não são exaustivas. Você deve analisar, avaliar, avaliar e aprovar a solução em conformidade com os recursos, ferramentas e configurações de segurança específicos da sua organização. É responsabilidade exclusiva de você e de sua organização determinar quais requisitos regulatórios são aplicáveis e garantir que

you meet all the requirements. Although this solution discusses technical and administrative requirements, it does not help you meet non-technical administrative requirements.

Planejando sua implantação do LZA em AWS

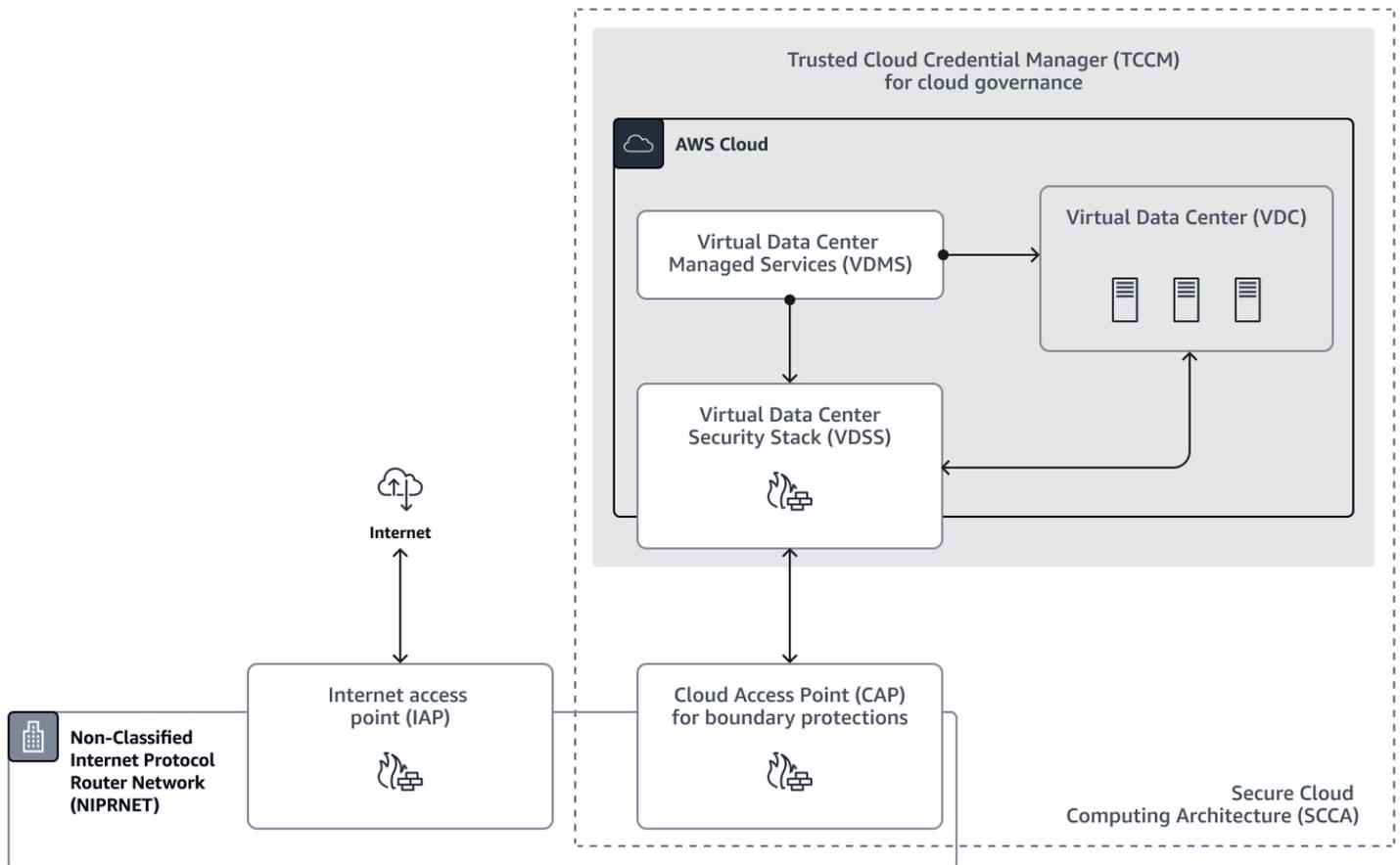
AWS created a [detailed implementation guide](#) for implementing the Landing Zone Accelerator (LZA) in AWS. To get an architecture diagram and a high-level overview of the implementation steps, consult the [architecture diagram](#) in the Landing Zone Accelerator in the AWS Implementation Guide. Your environment must meet the [prerequisites](#) before implementing the solution. Using the requirements in the components and prerequisites chapter of the SCCA of this guide, you can choose between the implementation options described in the [LZA implementation guide](#).

Componentes e requisitos do SCCA

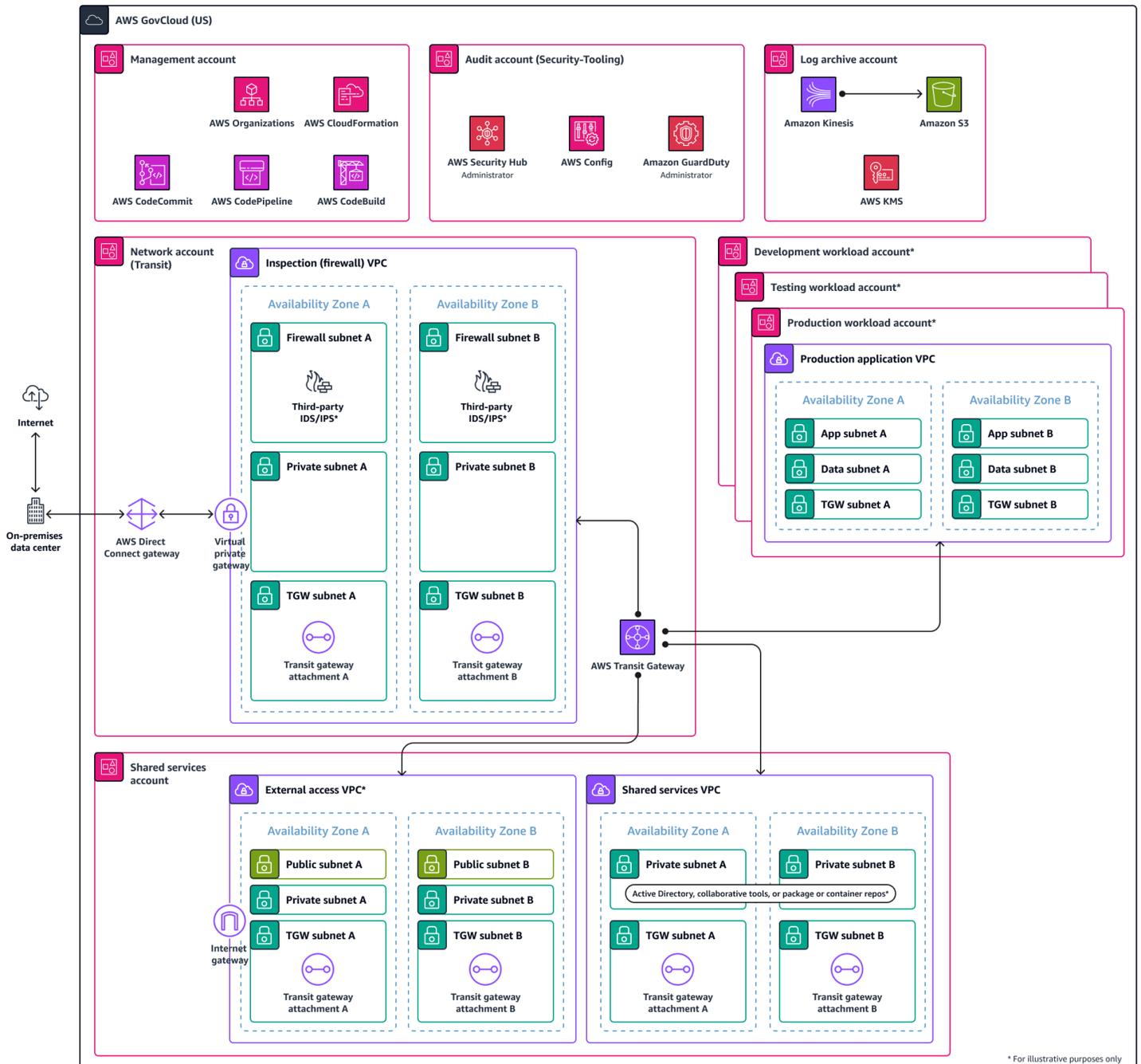
A Arquitetura de Computação em Nuvem Segura (SCCA) da Defense Information Systems Agency (DISA), adotada pelo Departamento de Defesa dos EUA (DoD), pretende ser uma abordagem escalável e econômica para proteger aplicativos baseados em nuvem sob uma arquitetura de segurança comum. Ele fornece uma abordagem padrão para proteger dados IL4 e IL5 em ambientes de nuvem. Conforme descrito na [ficha técnica do DISA SCCA](#), os componentes abrangentes do SCCA incluem:

- Ponto de acesso à nuvem (CAP) — fornece acesso à nuvem e protege as redes do DoD da nuvem. Proteções simplificadas com foco na proteção dos limites da rede.
- Virtual Data Center Security Stack (VDSS) — Segurança de enclave de rede virtual para proteger aplicativos e dados em ofertas comerciais de nuvem.
- Virtual Data Center Managed Services (VDMS) — Segurança do host de aplicativos para acesso privilegiado de usuários em ambientes comerciais.
- Trusted Cloud Credential Manager (TCCM) — Gerenciador de credenciais de nuvem para aplicar o controle de acesso baseado em funções (RBAC) e o acesso menos privilegiado.

A imagem a seguir mostra esses componentes do SCCA.



Esta seção discute cada componente em detalhes e os componentes correspondentes no LZA que podem ajudá-lo a aderir ao padrão da Agência de Sistemas de Informação de Defesa (DISA). A imagem a seguir mostra a estrutura de várias contas do LZA que cria os componentes do SCCA dentro do. Nuvem AWS Essa estrutura de várias contas do LZA é uma base que ajuda você a obter uma arquitetura totalmente compatível com os requisitos do DISA SCCA. Para ver um exemplo de uma arquitetura que ajuda você a atender totalmente aos requisitos de conformidade, consulte o [SCCA no diagrama de AWS GovCloud arquitetura](#).



Ponto de acesso à nuvem

O Boundary Cloud Access Point (BCAP) ou Cloud Access Point (CAP) é predeterminado pela sua organização. Portanto, não está no escopo deste guia. O CAP fornece acesso a ambientes comerciais de nuvem a partir da Rede de Sistemas de Informação de Defesa (DISN). O CAP também fornece proteção de limites do DISN da nuvem. No limite do DISN, ele inclui recursos de defesa cibernética, como firewall, sistemas de detecção de intrusões (IDS) e sistemas de prevenção

de intrusões (IPS). É comum que as organizações usem o [Design de Referência de Ponto de Acesso Nativo em Nuvem](#) do DoD para acessar. AWS

Pilha de segurança de data center virtual

O objetivo do Virtual Data Center Security Stack (VDSS) é proteger os aplicativos do proprietário da missão do DOD que estão hospedados em. AWS O VDSS fornece um enclave para serviços de segurança. O VDSS executa a maior parte das operações de segurança no SCCA. Esse componente contém serviços de segurança e rede, como controles de acesso à conectividade de entrada e serviços de proteção de perímetro, incluindo firewalls de aplicativos web, proteção contra DDOS, balanceadores de carga e recursos de roteamento de rede. O VDSS pode residir na infraestrutura de nuvem ou no local, em seu data center. AWS ou fornecedores terceirizados podem fornecer recursos de VDSS por meio de infraestrutura como serviço (IaaS) ou AWS podem oferecer esses recursos por meio de soluções de software como serviço (SaaS). Para obter mais informações sobre o VDSS, consulte o Guia de requisitos de segurança de [computação em nuvem do DoD](#).

A tabela a seguir contém os requisitos mínimos para o VDSS. Ele explica se o LZA atende a cada requisito e qual Serviços da AWS você pode usar para atender a esses requisitos.

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|---|---|--------------------------------------|------------------|
| 2.1.2.1 | O VDSS deve manter a separação virtual de todo o tráfego de gerenciamento, usuário e dados. | AWS Network Firewall Lista de controle de acesso à rede (ACL) Grupos de segurança para interfaces de rede elásticas | Isole VPCs | Coberto |
| 2.1.2.2 | O VDSS deve permitir o uso de criptografia | Amazon VPC (criptografe o | Melhores práticas de | Coberto |

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|--|---|---|----------------------|
| | para segmentação do tráfego de gerenciamento. | tráfego entre instâncias) | criptografia para Amazon VPC | |
| 2.1.2.3 | O VDSS deve fornecer um recurso de proxy reverso para lidar com solicitações de acesso de sistemas clientes. | N/D | Servir conteúdo usando um proxy reverso totalmente gerenciado | Não coberto |
| 2.1.2.4 | O VDSS deve fornecer a capacidade de inspecionar e filtrar conversas na camada de aplicação com base em um conjunto predefinido de regras (incluindo HTTP) para identificar e bloquear conteúdo malicioso. | AWS WAF Firewall de rede | Inspeção do corpo de solicitação da Web Inspeção de tráfego TLS com Network Firewall | Parcialmente coberto |

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|---|---|--|----------------------|
| 2.1.2.5 | O VDSS deve fornecer um recurso que possa distinguir e bloquear o tráfego não autorizado da camada de aplicação. | AWS WAF | Como usar a Amazon GuardDuty e AWS WAF para bloquear automaticamente hosts suspeitos | Não coberto |
| 2.1.2.6 | O VDSS deve fornecer um recurso que monitore as atividades da rede e do sistema para detectar e denunciar atividades maliciosas do tráfego que entra e sai das redes/ enclaves virtuais privados do Proprietário da Missão. | VPC Flow Logs Amazon GuardDuty AWS Enclaves Nitro | AWS Workshop Nitro Enclaves | Parcialmente coberto |

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|--|---|--|----------------------|
| 2.1.2.7 | O VDSS deve fornecer um recurso que monitore as atividades da rede e do sistema para interromper ou bloquear atividades maliciosas detectadas. | Firewall de rede AWS WAF | N/D | Parcialmente coberto |
| 2.1.2.8 | O VDSS deve inspecionar e filtrar o tráfego que passa entre as redes/encaves virtuais privados do proprietário da missão. | Firewall de rede | Implemente a filtragem de tráfego centralizada | Coberto |

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|----------|---|----------------------------------|--|------------------|
| 2.1.2.9 | O VDSS deve realizar a interrupção e inspeção do tráfego de comunicação SSL/TLS com suporte à autenticação única e dupla para tráfego destinado a sistemas hospedados no CSE. | Firewall de rede | Modelos de implantação para Network Firewall | Coberto |
| 2.1.2.10 | O VDSS deve fornecer uma interface para conduzir portas, protocolos e atividades de gerenciamento de serviços (PPSM) a fim de fornecer controle aos operadores de MCD. | Firewall de rede | Modelos de implantação para Network Firewall | Coberto |

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|----------|--|---|--|------------------|
| 2.1.2.11 | O VDSS deve fornecer um recurso de monitoramento que capture arquivos de log e dados de eventos para análise de segurança cibernética. | Amazon CloudWatch AWS CloudTrail | Registro para resposta a incidentes de segurança | Coberto |

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|----------|--|--|---|------------------|
| 2.1.2.12 | O VDSS deve fornecer ou alimentar informações de segurança e dados de eventos a um sistema de arquivamento alocado para coleta, armazenamento e acesso comuns aos registros de eventos por usuários privilegiados que realizam atividades do Boundary and Mission CND. | CloudWatch Registros da Amazon | Segurança em CloudWatch registros | Coberto |

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|----------|---|--|--|------------------|
| 2.1.2.13 | O VDSS deve fornecer um sistema de gerenciamento de chaves de criptografia compatível com FIPS-140-2 para armazenamento de credenciais de chave de criptografia privada de servidor geradas e atribuídas pelo DoD para acesso e uso pelo Web Application Firewall (WAF) na execução de quebra de SSL/TLS e inspeção de sessões de comunicação criptografadas. | AWS Secrets Manager AWS Key Management Service(AWS KMS) | Melhore a segurança de CloudFront origem da Amazon com AWS WAF o Secrets Manager AWS KMS gerenciamento de chaves com FIPS 140-2 | Não coberto |

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|----------|--|---|---------------------|------------------|
| 2.1.2.14 | O VDSS deve fornecer a capacidade de detectar e identificar o sequestro de sessões de aplicativos. | N/D | N/D | Não coberto |
| 2.1.2.15 | O VDSS fornecerá uma extensão DMZ do DoD para dar suporte a aplicativos voltados para a Internet (IFAs). | N/D | N/D | Não coberto |
| 2.1.2.16 | O VDSS deve fornecer captura completa de pacotes (FPC) ou capacidade de FPC equivalente ao serviço em nuvem para gravar e interpretar comunicações transversais. | Firewall de rede VPC Flow Logs | N/D | Coberto |

| ID | Requisito de segurança do VDSS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|----------|---|----------------------------------|---|------------------|
| 2.1.2.17 | O VDSS deve fornecer métricas e estatísticas de fluxo de pacotes de rede para todas as comunicações de travessia. | CloudWatch | Monitore a taxa de transferência de rede dos endpoints VPC da interface usando CloudWatch | Coberto |
| 2.1.2.18 | O VDSS deve prever a inspeção do tráfego que entra e sai da rede privada virtual de cada proprietário da missão. | Firewall de rede | Implemente a filtragem de tráfego centralizada | Coberto |

Há componentes do CAP que você define e que não são abordados neste guia porque cada agência tem sua própria conexão com o CAP AWS. Você pode complementar os componentes do VDSS com o LZA para ajudar a inspecionar o tráfego que entra. AWS Os serviços usados no LZA fornecem verificação de limites e tráfego interno para ajudar a proteger seu ambiente. Para continuar criando um VDSS, há alguns componentes adicionais de infraestrutura que não estão incluídos no LZA.

Ao usar a nuvem privada virtual (VPCs), você pode estabelecer limites em cada uma delas Conta da AWS para ajudar a aderir aos padrões da SCCA. Isso não é configurado como parte do LZA porque VPCs, endereçamento IP e roteamento são componentes que você deve configurar conforme necessário para sua infraestrutura. Você pode implementar componentes como Domain Name System Security Extensions (DNSSEC) no [Amazon Route 53](#). Você também pode adicionar WAFs comerciais AWS WAF ou de terceiros para ajudá-lo a atingir os padrões necessários.

Além disso, para suportar o requisito 2.1.2.7 no DISA SCCA, você pode usar o [Network GuardDutyFirewall](#) para ajudar a proteger e monitorar o ambiente em busca de tráfego mal-intencionado.

Managed Services de data center virtual

O objetivo do Virtual Data Center Managed Services (VDMS) é fornecer segurança ao host e serviços compartilhados de data center. As funções do VDMS podem ser executadas no hub do seu SCCA ou o proprietário da missão pode implantar partes dele por conta própria. Contas da AWS Esse componente pode ser fornecido em seu AWS ambiente. Para obter mais informações sobre o VDMS, consulte o Guia de requisitos de segurança de [computação em nuvem do DoD](#).

A tabela a seguir contém os requisitos mínimos para o VDMS. Ele explica se o LZA atende a cada requisito e qual Serviços da AWS você pode usar para atender a esses requisitos.

| ID | Requisito de segurança do VDMS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|--|---|--|----------------------|
| 2.1.3.1 | O VDMS deve fornecer uma Solução de Avaliação de Conformidade Assegurada (ACAS), ou equivalente aprovado, para conduzir o monitoramento contínuo de todos os enclaves dentro do CSE. | AWS Config AWS Security Hub AWS Audit Manager Amazon Inspector | Análise de vulnerabilidades com o Amazon Inspector | Parcialmente coberto |
| 2.1.3.2 | O VDMS deve fornecer um | N/D | N/D | Não coberto |

| ID | Requisito de segurança do VDMS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|----|---|-----------------|---------------------|------------------|
| | Sistema de Segurança Baseado em Host (HBSS), ou equivalente aprovado, para gerenciar a segurança de terminais para todos os enclaves dentro do CSE. | | | |

| ID | Requisito de segurança do VDMS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|---|---|---|----------------------|
| 2.1.3.3 | O VDMS deve fornecer serviços de identidade e para incluir um respondente do Online Certificate Status Protocol (oCloud Workload Security) para autenticação de dois fatores do Cartão de Acesso Comum (CAC) do DoD de sistemas remotos de usuários privilegiados do DoD em sistemas instanciados no CSE. | <p>Autenticação multifatorial (MFA) disponível por meio de:</p> <p>AWS Identity and Access Management (IAM)</p> <p>AWS IAM Identity Center</p> <p>AWS Directory Service for Microsoft Active Directory</p> <p>AWS Private Certificate Authority</p> | Configurar um cartão CAC para a Amazon WorkSpaces | Parcialmente coberto |

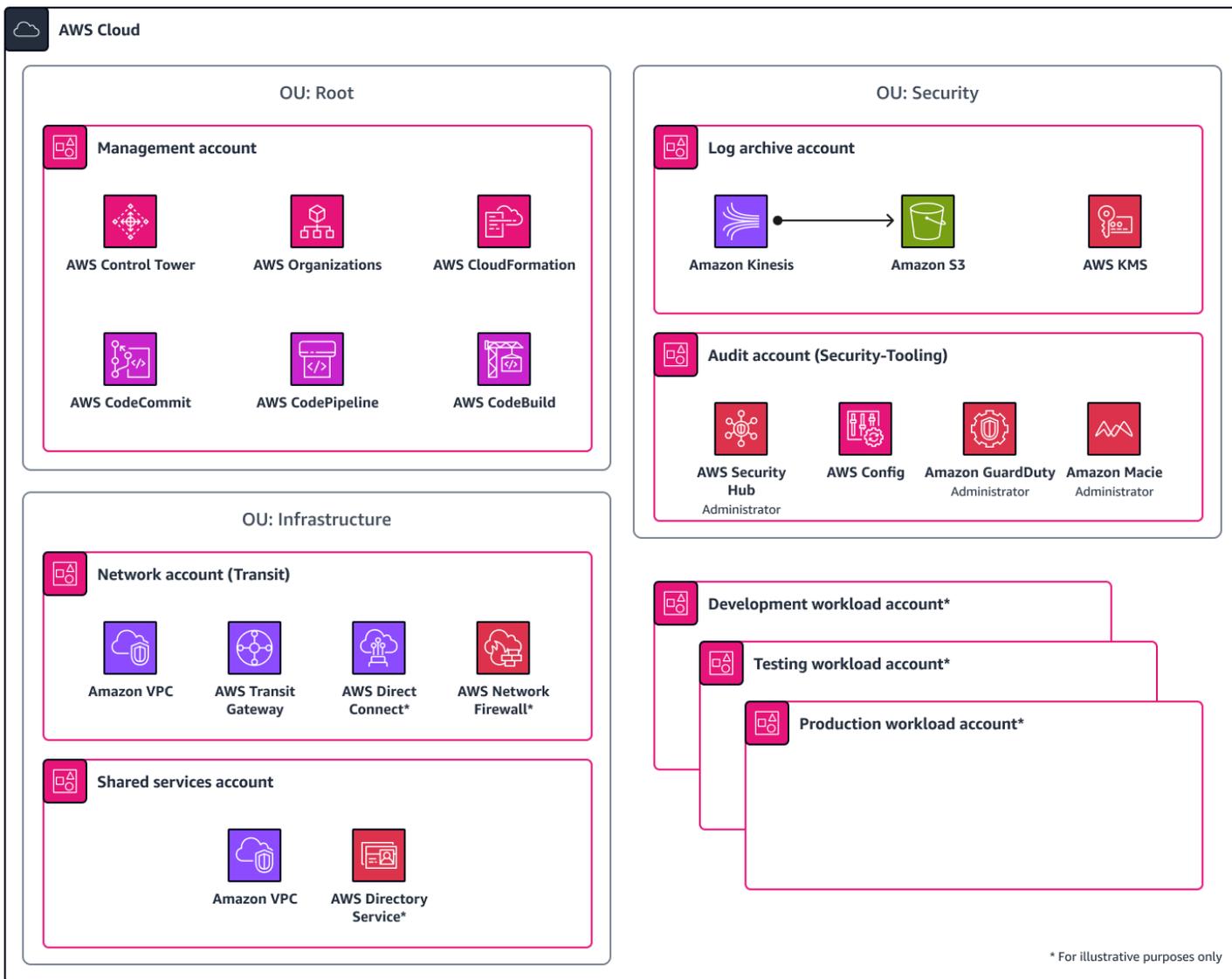
| ID | Requisito de segurança do VDMS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|---|--|--|----------------------|
| 2.1.3.4 | O VDMS deve fornecer um sistema de gerenciamento de configuração e atualização para atender sistemas e aplicativos para todos os enclaves dentro do CSE. | AWS Systems Manager Patch Manager AWS Config | Automatizando o gerenciamento de patches com AWS Systems Manager(vídeo) YouTube | Parcialmente coberto |
| 2.1.3.5 | O VDMS deve fornecer serviços de domínio lógico para incluir acesso a diretórios, federações, diretórios, Protocolo de Configuração Dinâmica de Host (DHCP) e Sistema de Nomes de Domínio (DNS) para todos os enclaves dentro do CSE. | AWS Managed Microsoft AD Amazon Virtual Private Cloud (Amazon VPC) Amazon Route 53 | Configurar atributos de DNS para sua VPC | Parcialmente coberto |

| ID | Requisito de segurança do VDMS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|--|---|---------------------|------------------|
| 2.1.3.6 | O VDMS deve fornecer uma rede para gerenciar sistemas e aplicativos dentro do CSE que seja logicamente separada das redes de usuários e dados. | Amazon VPC Sub-redes da Amazon VPC | N/D | Coberto |

| ID | Requisito de segurança do VDMS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|---|---|--|------------------|
| 2.1.3.7 | O VDMS deve fornecer um sistema, segurança, aplicativo e sistema de arquivamento de eventos de atividades do usuário para coleta, armazenamento e acesso comuns aos registros de eventos por usuários privilegiados que realizam atividades de BCP e MCP. | AWS Security Hub AWS CloudTrail CloudWatch Registros da Amazon Amazon Simple Storage Service (Amazon S3) | Registro centralizado com OpenSearch | Coberto |

| ID | Requisito de segurança do VDMS | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|--|--|--|----------------------|
| 2.1.3.8 | O VDMS deve fornecer a troca de atributos de autenticação e autorização de usuários privilegiados do DoD com o sistema de gerenciamento de identidade e acesso do CSP para permitir o provisionamento, a implantação e a configuração do sistema em nuvem. | AWS Managed Microsoft AD | Melhore sua configuração AWS Managed Microsoft AD de segurança | Não coberto |
| 2.1.3.9 | O VDMS deve implementar as capacidades técnicas necessárias para executar a missão e os objetivos da função do TCCM. | AWS Managed Microsoft AD IAM IAM Identity Center | N/D | Parcialmente coberto |

Conforme mostrado na imagem a seguir, o LZA estabelece os componentes fundamentais para atender aos requisitos básicos do VDMS. Há alguns componentes adicionais que você precisa configurar após a implantação do LZA para ajudá-lo a atender aos padrões do VDMS. Na tabela anterior, verifique os links na coluna Recursos adicionais. Esses links ajudam você a configurar esses itens adicionais ou fornecem mais aprimoramentos de segurança.



Integração de serviços suplementares

A coluna Recursos adicionais da tabela anterior lista recursos para ajudá-lo a expandir o LZA para atender aos requisitos do VDMS. Além disso, oferece alguns materiais de workshop para ajudá-lo a configurar uma arquitetura de nuvem segura. Sem modificações, o LZA atende aos

requisitos de IL4/IL5, mas você pode implantar serviços adicionais para aprimorar a segurança do seu ambiente. AWS

Por exemplo, o Amazon Inspector é um serviço de gerenciamento de vulnerabilidades que verifica continuamente suas AWS cargas de trabalho em busca de vulnerabilidades de software e exposição não intencional na rede. Você pode usá-lo para identificar e investigar vulnerabilidades em sistemas operacionais hospedeiros, como Windows e Linux. Embora o Amazon Inspector possa não incorporar totalmente todos os requisitos necessários para um Sistema de Segurança Baseado em Host (HBSS), ele fornece pelo menos uma avaliação básica da vulnerabilidade das instâncias.

Patches do sistema operacional.

A correção do sistema operacional é um componente essencial da operação de um ambiente seguro. AWS oferece e recomenda o uso do [Patch Manager](#), um recurso do AWS Systems Manager, para manter linhas de base de patches consistentes e automatizar a implantação de patches. O Patch Manager automatiza o processo de correção de nós gerenciados com atualizações relacionadas à segurança e outros tipos de atualizações.

Você pode usar o Patch Manager para aplicar patches de sistemas operacionais e aplicativos. (No Windows Server, o suporte a aplicativos é limitado às atualizações de aplicativos lançados pela Microsoft.) Para obter mais informações, consulte [Orquestração de processos de patch personalizados em várias etapas usando o AWS Systems Manager Patch Manager no blog](#) de operações e migrações na AWS nuvem.

Para step-by-step obter instruções sobre como usar o Patch Manager, consulte o [Workshop de Ferramentas AWS de Gerenciamento e Governança](#).

Para obter mais informações sobre como proteger cargas de trabalho do Microsoft Windows em AWS, consulte [Protegendo cargas de trabalho do Windows no Workshop](#). AWS

Gerenciador de credenciais de nuvem confiável

O Trusted Cloud Credential Manager (TCCM) é um componente do SCCA. É responsável pelo gerenciamento de credenciais. Ao estabelecer o TCCM, é importante permitir o acesso com [privilégios mínimos ao SCCA](#). Isso pode ser feito usando serviços de gerenciamento de AWS identidade e acesso. Um componente adicional do TCCM é uma conexão com o Virtual Data Center Managed Services (VDMS). Você pode usar essa conexão conforme necessário para acessar o AWS Management Console para gerenciar o TCCM.

O TCCM é uma combinação de tecnologias e padrões que regem o acesso a AWS. O TCCM é considerado essencial para a maioria das implementações porque controla as permissões de acesso. A função TCCM não se destina a impor requisitos exclusivos de gerenciamento de identidade ao provedor comercial de serviços em nuvem (CSP). O TCCM também não proíbe o uso da federação de CSP do DoD ou de soluções de intermediação de identidade de terceiros para fornecer o controle de identidade pretendido.

Os componentes da política do TCCM são baseados em um entendimento geral de que os CSPs oferecem um sistema de gerenciamento de identidade e acesso que permite o controle do acesso aos sistemas em nuvem. Esses sistemas podem incluir o console de acesso, a API e os componentes de serviço da interface de linha de comando (CLI) do CSP. No nível básico, o TCCM deve bloquear as credenciais que podem ser usadas para criar redes não autorizadas e outros recursos. O TCCM é nomeado pelo Oficial Autorizador (AO) encarregado de supervisionar os sistemas de TI. As políticas do TCCM estabelecem a necessidade de um modelo de acesso com privilégios mínimos. Essas políticas são responsáveis pelo fornecimento e controle de credenciais de usuários privilegiados na nuvem comercial. Isso é para se manter alinhado com o Guia de [Requisitos de Segurança de Computação em Nuvem do DoD](#), que aborda a implementação de políticas, planos e procedimentos para gerenciar suas credenciais de conta do portal. [Antes da conexão com a Rede de Sistemas de Informação de Defesa \(DISN\), a DISA valida a existência do Plano de Gerenciamento de Credenciais de Nuvem \(CCMP\) como parte do processo de aprovação de conexão definido no Guia do Processo de Conexão.](#)

A tabela a seguir contém os requisitos mínimos para o TCCM. Ele explica se o LZA atende a cada requisito e qual Serviço da AWS você pode usar para atender a esses requisitos.

| ID | Requisitos de segurança do TCCM | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|---|-----------------|---------------------|------------------|
| 2.1.4.1 | O TCCM desenvolverá e manterá um Plano de Gerenciamento de Credenciais em Nuvem (CCMP) para | N/D | N/D | Não coberto |

| ID | Requisitos de segurança do TCCM | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|---|---|---------------------|------------------|
| | abordar a implementação de políticas, planos e procedimentos que serão aplicados ao gerenciamento de credenciais da conta do portal do cliente do proprietário da missão. | | | |
| 2.1.4.2 | O TCCM deve coletar, auditar e arquivar todos os registros e alertas de atividades do Portal do Cliente. | AWS CloudTrail CloudWatch Registros da Amazon | N/D | Coberto |

| ID | Requisitos de segurança do TCCM | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|---|---|---------------------|------------------|
| 2.1.4.3 | O TCCM deve garantir que os alertas do registro de atividades sejam compartilhados, encaminhados ou recuperáveis por usuários privilegiados do DoD envolvidos em atividades de MCP e BCP. | AWS CloudTrail CloudWatch Registros Amazon Simple Notification Service (Amazon SNS) CloudWatch Informações sobre registros | N/D | Coberto |

| ID | Requisitos de segurança do TCCM | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|--|--|---------------------|------------------|
| 2.1.4.4 | O TCCM deve, conforme necessário para o compartilhamento de informações, criar contas de acesso ao repositório de registros para acesso aos dados do registro de atividades por usuários privilegiados que realizam atividades de MCP e BCP. | AWS CloudTrail CloudWatch Registros Amazon SNS CloudWatch Informações sobre registros | N/D | Coberto |
| 2.1.4.5 | O TCCM deve recuperar e controlar com segurança as credenciais da conta do portal do cliente antes da conectividade do aplicativo da missão com o DISN. | AWS IAM Identity Center | N/D | Coberto |

| ID | Requisitos de segurança do TCCM | AWS tecnologias | Recursos adicionais | Coberto pela LZA |
|---------|---|--|---------------------|------------------|
| 2.1.4.6 | O TCCM deve criar, emitir e revogar, conforme necessário, credenciais de acesso menos privilegiado do portal do cliente baseado em funções para administradores de aplicativos e sistemas do proprietário da missão (ou seja, usuários privilegiados do DoD). | AWS Identity and Access Management (IAM) AWS Directory Service for Microsoft Active Directory | N/D | Coberto |

Para permitir que o TCCM atenda aos requisitos, o LZA usa o controle programático dos recursos por meio do serviço IAM. Além disso, você pode combinar o IAM com AWS Managed Microsoft AD para implementar o login único em outro diretório. Isso vincula seu AWS ambiente à sua infraestrutura local com relações de confiança do Active Directory. No LZA, a implementação é implantada com funções do IAM para acesso temporário baseado em sessão. As funções do IAM são credenciais de curta duração que ajudam sua organização a atender aos requisitos necessários do TCCM.

Embora o LZA implemente o acesso com privilégios mínimos e o acesso programático de curto prazo aos AWS recursos, analise as [melhores práticas do IAM](#) para garantir que você siga as diretrizes de segurança recomendadas.

Para obter mais informações sobre a implementação AWS Managed Microsoft AD, consulte a [AWS Managed Microsoft AD](#) seção do workshop do Active Directory no AWS Immersion Day.

O [modelo de responsabilidade AWS compartilhada](#) se aplica ao TCCM e ao LZA. O LZA cria os aspectos fundamentais do controle de acesso, mas cada organização é responsável pela configuração de seus controles de segurança.

Conclusão

Para o Departamento de Defesa dos EUA (DoD), este guia explica quais são os requisitos da Agência de Sistemas de Informação de Defesa (DISA) para implantar uma Arquitetura de Computação em Nuvem Segura (SCCA). Ao usar o Landing Zone Accelerator (LZA) ativado AWS, você pode implementar AWS ofertas e eliminar o trabalho pesado indiferenciado. Isso ajuda você a se concentrar em sua missão de criar uma infraestrutura de nuvem compatível com IL4 ou IL5.

Recursos

AWS documentação

- [AWS Serviços no escopo do Programa de Conformidade](#) (AWS Conformidade)
- [Guia de requisitos de segurança de computação em nuvem do Departamento de Defesa](#) (AWS conformidade)
- [Landing Zone Accelerator ativado AWS](#) (Biblioteca de AWS soluções)
- [Guia de AWS implementação do Landing Zone Accelerator](#)
- [SCCA no diagrama de AWS GovCloud arquitetura](#)

Outros recursos

- [Guia de requisitos de segurança de computação em nuvem](#) (site da DISA)
- [Projeto de referência do ponto de acesso nativo em nuvem \(CNAP\) do Departamento de Defesa \(DoD\)](#) (site do DoD)
- [Ficha técnica da arquitetura de computação em nuvem segura do DoD](#) (site da DISA)

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 |
|------------------------------------|-----------|---------------------|
| Publicação inicial | — | 12 de março de 2024 |

AWS Glossário de Recomendações da

Os termos a seguir são comumente usados em estratégias, guias e padrões fornecidos pelas AWS Recomendações da. Para sugerir entradas, use o link [Fornecer feedback](#) no final do glossário.

Números

7 Rs

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

- **Refatorar/rearquitetar:** mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Aurora SQL Edição Compatível com Postgre.
- **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: migrar seu banco de dados Oracle on-premises para o Amazon Relational Database Service (AmazonRDS) para Oracle no. Nuvem AWS
- **Recomprar (drop and shop):** mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migrar seu sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
- **Redefinir a hospedagem (mover sem alterações [lift-and-shift])** mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: migrar seu banco de dados Oracle on-premises para o Oracle em uma EC2 instância no. Nuvem AWS
- **Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]):** mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma local para um serviço em nuvem para a mesma plataforma. Exemplo: Migrar um Microsoft Hyper-V aplicativo para AWS.
- **Rever (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

Veja 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. Ele é mais flexível, mas exige mais trabalho do que a migração [ativa-passiva](#).

migração ativa-passiva

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

função agregada

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

AI

Veja a [inteligência artificial](#).

AIOps

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

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade () ACID

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

controle de acesso baseado em atributos () ABAC

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

fonte de dados autorizada

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

Availability Zone (zona de disponibilidade)

Um local distinto em uma Região da AWS que é isolado das falhas em outras zonas de disponibilidade e fornece conectividade de rede de baixa latência e baixo custo para outras zonas de disponibilidade na mesma região.

AWS Estrutura de adoção da nuvem (AWS CAF)

Uma estrutura de diretrizes e práticas recomendadas da AWS para ajudar as organizações a desenvolverem um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS CAF organiza a orientação em seis áreas de foco chamadas perspectivas: negócios, pessoas, 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. Para essa perspectiva, AWS CAF fornece orientação para desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o [AWS CAFsite](#) e o [AWS CAFwhitepaper](#).

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

Uma ferramenta que avalia os workloads de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS WQF está incluído com AWS Schema

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

B

bot inválido

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, API chamadas 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 canário

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

Consulte [Centro de Excelência da Nuvem](#).

CDC

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

captura de dados de alteração (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 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 [integração contínua e entrega contínua](#).

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 feita localmente, antes que o de destino os AWS service (Serviço da AWS) receba.

Centro de Excelência da Nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendadas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as [CCoEpublicações](#) 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 é comumente 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 ao migrar para o Nuvem AWS:

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação: realizar investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma landing zone, definir uma CCoE, estabelecer um modelo de operações)

- Migração: migrar aplicações individuais
- Reinvenção: otimizar produtos e serviços e inovar na nuvem

Esses estágios foram definidos por Stephen Orban na publicação no blog A [jornada rumo à nuvem em primeiro lugar e os estágios da adoção no Blog de estratégia Nuvem AWS](#) empresarial. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração da, consulte o [guia de preparação para migração](#).

CMDB

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

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja [visão computacional](#).

D

dados em repouso

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

classificação de dados

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

desvio de dados

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

dados em trânsito

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

Malha de dados

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

minimização de dados

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

perímetro de dados

Um conjunto de barreiras preventivas em seu AWS ambiente da 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 na AWS, você adiciona vários controles em diferentes camadas da AWS Organizations estrutura do para ajudar a proteger os recursos. Por exemplo, uma defense-in-depth abordagem pode combinar autenticação multifatorial, segmentação de rede e criptografia.

administrador delegado

No AWS Organizations, um serviço compatível pode registrar uma AWS conta-membro da para administrar as contas da organização e gerenciar permissões para esse serviço. Essa conta

é chamada de administrador delegado para esse serviço Para obter mais informações e uma lista de serviços compatíveis, consulte [Serviços que funcionam com o AWS Organizations](#) na documentação do AWS Organizations .

implantação

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

ambiente de desenvolvimento

Veja o [ambiente](#).

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

A estratégia e o processo que você usa para minimizar o tempo de inatividade e a perda de dados causados por um [desastre](#). Para obter mais informações, consulte [Recuperação de Workloads em Desastres em AWS: Recuperação na Nuvem na 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 modernizar modernizar modernizar modernizar a Microsoft herdada. ASP NET\(ASMX\) serviços web incrementalmente usando contêineres e Amazon API Gateway.](#)

DR

Veja a [recuperação de desastres](#).

detecção de desvios

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 de desenvolvimento](#).

E

EDA

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

computação de borda

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

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o [endpoint do serviço](#).

serviço de endpoint

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

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

environment (ambiente)

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

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

epic

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

ERP

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

análise exploratória de dados () EDA

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

detectar anomalias e verificar suposições. EDA é realizado por meio do cálculo de estatísticas resumidas e da criação de visualizações de dados.

F

tabela de fatos

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

falhar rápido

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 machine learning com:AWS](#).

transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único

campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo, se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

FGAC

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

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 de alterações](#) para migrar os dados no menor tempo possível, em vez de usar uma abordagem em fases. O objetivo é reduzir ao mínimo o tempo de inatividade.

G

bloqueio geográfico

Veja as [restrições geográficas](#).

restrições geográficas (bloqueio geográfico)

Na Amazon CloudFront, uma opção para impedir que usuários em países específicos acessem distribuições de conteúdo. É possível usar uma lista de permissões ou uma lista de bloqueios para especificar países aprovados e banidos. Para obter mais informações, consulte [Como restringir a distribuição geográfica de 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 antigo, e o fluxo de [trabalho baseado em troncos](#) é a abordagem moderna e preferida.

estratégia greenfield

A ausência de infraestrutura existente em um novo ambiente. Ao adotar uma estratégia greenfield para uma arquitetura de sistema, é possível selecionar todas as novas tecnologias sem a

restrição da compatibilidade com a infraestrutura existente, também conhecida como [brownfield](#). Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

barreira de proteção

Uma regra de alto nível que ajuda a gerenciar recursos, políticas e conformidade em todas as unidades organizacionais (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 IAM permissões. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a [alta disponibilidade](#).

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

I

IaC

Veja a [infraestrutura como código](#).

Política baseada em identidade

Uma política associada a uma ou mais IAM entidades principais que define suas permissões dentro do Nuvem AWS ambiente da.

aplicação ociosa

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

IloT

Veja [Internet das Coisas Industrial \(IIoT\)](#).

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. [As infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que as mutáveis.](#) Para obter mais informações, consulte as práticas recomendadas para [implantar usando infraestrutura imutável](#) no Well-Architected AWS Framework.

admissão (admissão) VPC

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

migração incremental

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

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet das Coisas Industrial (IIoT)

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

inspeção VPC

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

Internet das Coisas (IoT)

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

interpretabilidade

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

IoT

Consulte [Internet das Coisas](#).

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

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

ITSM

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

L

controle de acesso baseado em 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 da com várias contas que é bem arquitetado, escalável e seguro. Um ponto a partir do qual suas organizações podem iniciar e implantar rapidamente workloads e aplicações com confiança em seu ambiente de segurança e infraestrutura. Para obter mais informações sobre zonas de pouso, consulte [Configurar um ambiente da AWS com várias contas seguro e escalável](#).

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

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

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja [7 Rs](#).

sistema little-endian

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

ambientes inferiores

Veja o [ambiente](#).

M

machine learning (ML)

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

ramificação principal

Veja a [filial](#).

malware

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

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte [Migration Acceleration Program](#).

mecanismo

Um processo completo no qual você cria uma ferramenta, impulsiona a adoção da ferramenta e, em seguida, inspeciona os resultados para fazer ajustes. Um mecanismo é um ciclo que se

reforça e se aprimora à medida que opera. Para obter mais informações, consulte [Construir mecanismos](#) no AWS Well-Architected Framework.

conta-membro

Todas as, Contas da AWS exceto a conta de gerenciamento que faz parte de uma organização no AWS Organizations. Uma conta só pode ser membro de uma organização de cada vez.

MES

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

Transporte de telemetria de enfileiramento de mensagens () MQTT

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

microsserviço

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

arquitetura de microsserviços

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

Programa de Aceleração da Migração (MAP)

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

migração em escala

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

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações, analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais trabalhando 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 de destino, o grupo de segurança e AWS conta da.

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: redefina a hospedagem da migração para a Amazon EC2 com o AWS Application Migration Service da.

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

O processo de obter insights sobre o status de preparação de uma organização para a nuvem, identificando pontos fortes e fracos e criar um plano de ação para fechar as lacunas identificadas

usando o AWS CAF Para mais informações, consulte o [guia de preparação para migração](#).
MRA é a primeira fase da [estratégia de AWS migração para a](#)

estratégia de migração

A abordagem usada para migrar um workload para a 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 aplicações no Nuvem AWS](#).

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte [Avaliar a prontidão para modernização de aplicações](#) no Nuvem AWS

aplicações monolíticas (monólitos)

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

MPA

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

MQTT

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

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

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

OAI

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

OCM

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

migração offline

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

OI

Veja a [integração de operações](#).

OLA

Consulte acordo de [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. 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 AWS Well-Architected Framework.

tecnologia operacional (OT)

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

integração de operações (OI)

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

trilha organizacional

Uma trilha criada pelo AWS CloudTrail que registra todos os eventos para todas as Contas da AWS em uma organização no 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 [Criar 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. 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 para a, essa estrutura é chamada de aceleração de pessoas devido à velocidade das alterações exigida nos projetos de adoção da nuvem. Para obter mais informações, consulte o [OCMguia](#).

controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo no Amazon Simple Storage Service (Amazon Simple Service). OAC oferece suporte a todos os buckets do S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e dinâmica PUT e DELETE solicitações ao bucket do S3.

Identidade do acesso de origem (OAI)

Dentro CloudFront, uma opção para restringir o acesso com o objetivo de proteger seu conteúdo no Amazon S3. Quando você usa OAI, CloudFront cria um principal com o qual o Amazon S3 pode se autenticar. As entidades principais autenticadas podem acessar 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](#).

NÃO

Veja a [tecnologia operacional](#).

de saída (egresso) VPC

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

P

limite de permissões

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

informações de identificação pessoal () PII

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

PII

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

manual

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

PLC

Consulte [controlador lógico programável](#).

PLM

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

política

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

persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um microsserviço com base em padrões de acesso a dados e outros requisitos. Se seus microsserviços tiverem a mesma tecnologia de armazenamento de dados, eles poderão enfrentar desafios de

implementação ou apresentar baixa performance. Os microsserviços serão implementados com mais facilidade e alcançarão performance e escalabilidade melhores se usarem o armazenamento de dados mais bem adaptado às suas necessidades. Para obter mais informações, consulte [Habilitar a persistência de dados em microsserviços](#).

avaliação do portfólio

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

predicado

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

passagem direta 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 deverão ser recuperados e processados no banco de dados relacional e melhora o desempenho da consulta.

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

Privacidade por design

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

zonas hospedadas privadas

Um contêiner que armazena informações sobre como você quer que o Amazon Route 53 responda a DNS consultas para um domínio e seus subdomínios dentro de 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 evitar a implantação de recursos fora de conformidade. Esses controles examinam os recursos antes de serem provisionados. Se o recurso não estiver em conformidade com o controle, ele não será provisionado. Para obter mais informações, consulte o [guia de referência de controles](#) na AWS Control Tower documentação e consulte [Controles proativos](#) em Implementação de controles de segurança em AWS.

gerenciamento do ciclo de vida do produto () PLM

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

ambiente de produção

Veja o [ambiente](#).

controlador lógico programável () PLC

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

pseudonimização

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

publicar/assinar (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

RACIMatriz

Veja [responsável, accountable, consultada, informada \(\) RACI](#).

ransomware

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

RASCIMatriz

Veja [responsável, accountable, consultada, informada \(\) RACI](#).

RCAC

Veja [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.

redefinir arquitetura

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 da em uma área geográfica. Cada Região da AWS é isolada e independente das demais 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 RASCImatriz e, se excluir, será chamada de RACImatriz.

controle responsivo

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

reter

Veja [7 Rs](#).

aposentar-se

Veja [7 Rs](#).

rotação

O processo em que você atualiza periodicamente o [segredo](#) para dificultar o acesso de um invasor às credenciais.

controle de acesso por linha e coluna (RCAC)

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

RPO

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

RTO

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

runbook

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

S

SAML2.0

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

IAM

SCADA

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

SCP

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

secret

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

controle de segurança

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

fortalecimento da segurança

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

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

Ferramentas e serviços que combinam sistemas de gerenciamento de informações de segurança (SIM) e gerenciamento de eventos de segurança (SEM). Um SIEM sistema coleta, monitora

e analisa dados de servidores, redes, dispositivos e outras fontes para detectar ameaças e violações de segurança e gerar alertas.

automação de resposta de segurança

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

Criptografia do lado do servidor

Criptografia dos dados no destino pelo AWS service (Serviço da AWS) que os recebe.

política de controle de serviço (SCP)

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

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

ponto único de falha (SPOF)

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

SLA

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

SLI

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

SLO

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

split-and-seed modelo

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

SPOF

Veja [um único ponto de falha](#).

esquema star

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 modernizar modernizar modernizar modernizar a Microsoft ASP herdada. NET\(ASMX\) serviços web incrementalmente usando contêineres e Amazon API Gateway](#).

sub-rede

Um intervalo de endereços IP no seu VPC. Cada sub-rede fica alocada em uma única zona de disponibilidade.

controle de supervisão e aquisição de dados () SCADA

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o [ambiente](#).

treinamento

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

gateway de trânsito

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

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 no 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 pode ser alimentada com duas pizzas. Uma equipe de duas pizzas garante a melhor oportunidade possível de colaboração no desenvolvimento de software.

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o [ambiente](#).

V

aspiração

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

controle de versões

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

VPCespiando

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do

projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

WORM

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

WQF

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

escreva uma vez, leia muitos (WORM)

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

Z

exploração de dia zero

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

vulnerabilidade de dia zero

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

aplicação zumbi

Uma aplicação que tem um uso médio CPU de 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.