Implementando uma estratégia de controle de bots em AWS

AWS Orientação prescritiva

AWS Orientação prescritiva: Implementando uma estratégia de controle de bots em AWS

Table of Contents

Implementando uma estratégia de controle de bots em AWS

Amazon Web Services (colaboradores)

Fevereiro de 2024 (histórico do documento)

A internet como a conhecemos não seria possível sem bots. Os bots executam tarefas automatizadas pela Internet e simulam a atividade ou interação humana. Eles permitem que as empresas criem eficiência em processos e tarefas. Bots úteis, como rastreadores da web, indexam informações na Internet e nos ajudam a encontrar rapidamente as informações mais relevantes para nossas consultas de pesquisa. Os bots são um bom mecanismo para melhorar os negócios e agregar valor às empresas. No entanto, com o tempo, os malfeitores começaram a usar bots como um meio de abusar dos sistemas e aplicativos existentes de maneiras novas e criativas.

As redes de bots são o mecanismo mais conhecido para escalar bots e seu impacto. As redes de bots são redes de bots infectadas por malware e estão sob o controle de uma única parte, conhecida como pastor de bots ou operador de bots. A partir de um ponto central, o operador pode comandar cada computador em seu botnet para realizar simultaneamente uma ação coordenada, razão pela qual os botnets também são chamados de sistemas command-and-control (C2).

A escala de uma botnet pode ser de muitos milhões de bots. Um botnet ajuda o operador a realizar ações em grande escala. Como os botnets permanecem sob o controle de um operador remoto, as máquinas infectadas podem receber atualizações e mudar seu comportamento rapidamente. Como resultado, para obter ganhos financeiros significativos, os sistemas C2 podem alugar o acesso a segmentos de sua botnet no mercado negro.

A prevalência de botnets continuou a crescer. É considerado pelos especialistas como a ferramenta favorita dos malfeitores. A Mirai é uma das maiores redes de bots. Surgiu em 2016, ainda está operacional e estima-se que tenha infectado até 350.000 dispositivos da Internet das Coisas (IoT). Esse botnet foi adaptado e usado para muitos tipos de atividades, incluindo ataques distribuídos de negação de serviço (DDoS). Mais recentemente, agentes mal-intencionados tentaram ofuscar ainda mais suas atividades e obter tráfego obtendo endereços IP por meio do uso de serviços de proxy residenciais. Isso cria um peer-to-peer sistema interconectado legítimo que adiciona sofisticação à atividade e torna mais difícil detectá-la e mitigá-la.

Este documento se concentra no cenário de bots, seu efeito em seus aplicativos e nas estratégias e opções de mitigação disponíveis. Essa orientação prescritiva e suas melhores práticas ajudam você a entender e mitigar os diferentes tipos de ataques de bots. Além disso, este guia descreve

os Serviços da AWS recursos que dão suporte a uma estratégia de mitigação de bots e como cada um deles pode ajudar você a proteger seus aplicativos. Também inclui uma visão geral do monitoramento de bots e das melhores práticas para otimizar os custos da solução.

Entendendo as ameaças e as operações dos bots

De acordo com a Security Today, mais de 47% de todo o tráfego na internet é devido a bots. Isso inclui a parte útil dos bots, aqueles que se identificam e fornecem valor. Cerca de 30% do tráfego de bots são bots não identificados que estão realizando atividades maliciosas, como ataques de DDoS, escalonamento de tíquetes, coleta de inventário ou acumulação. A Security Magazine relata um aumento de 300% nos eventos volumétricos de DDoS durante o primeiro semestre de 2023. Isso torna esse tópico mais relevante e torna o conhecimento sobre as ferramentas e tecnologias preventivas e de proteção disponíveis ainda mais importante.

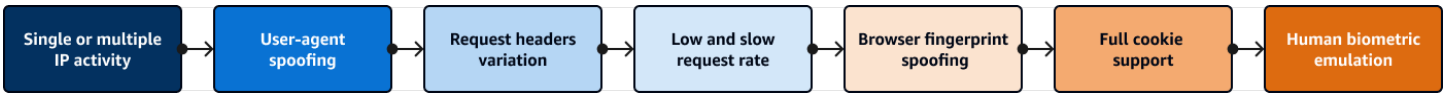
A tabela a seguir categoriza os diferentes tipos de atividades de bots e o impacto comercial que cada uma pode ter. Essa não é uma lista extensa; é um resumo das atividades mais comuns dos bots. Ele destaca a importância dos controles de monitoramento e mitigação. Para obter uma lista extensa de ameaças de bots, visite o manual de ameaças automatizadas a aplicativos da OWASP (site da OWASP).

Tipo de atividade do bot	Descrição	Impacto potencial
Raspagem de conteúdo	Cópia de conteúdo proprietá rio para uso em sites de terceiros	Impacto em seu SEO devido à duplicação de conteúdo, impacto na marca e problemas de desempenh o causados por raspadores agressivos
Preenchimento de credenciais	Teste de bancos de dados de credenciais roubadas em seu site para obter acesso ou validar informações	Problemas para os usuários, como fraudes e bloqueios de contas, que aumentam as consultas de suporte e diminuem a confiança na marca
Quebra de cartas	Testando bancos de dados de dados de cartões de crédito roubados para validar ou complementar as informações ausentes	Problemas para os usuários, como roubo de identidad e e fraude, e danos à sua pontuação de fraude

Tipo de atividade do bot	Descrição	Impacto potencial
Negação de serviço	Aumentar o tráfego para um site específico para diminuir a resposta ou torná-lo indisponí vel para tráfego legítimo	Perda de receita e danos à reputação
Criação de conta	Criação de várias contas com o objetivo de uso indevido ou ganho financeiro	Crescimento impedido e análise de marketing distorcid a
Escalpelamento	Obtenção de produtos com disponibilidade limitada, frequentemente ingressos , em vez de consumidores genuínos	Perda de receita e problemas para os usuários, como falta de acesso aos produtos vendidos

Como as botnets operam

As táticas, técnicas e procedimentos (TTP) dos operadores de botnets evoluíram substancialmente ao longo do tempo. Eles tiveram que acompanhar as tecnologias de detecção e mitigação desenvolvidas pelas empresas. A figura a seguir mostra essa evolução. As botnets começaram simplesmente usando endereços IP como meio de operação e, eventualmente, evoluíram para usar emulação biométrica humana sofisticada. Essa sofisticação é cara e nem todas as redes de bots usam as ferramentas mais avançadas. Há uma mistura de operadoras na Internet e elas provavelmente avaliam a melhor ferramenta para o trabalho para proporcionar um bom retorno sobre o investimento. Um objetivo na defesa de bots é tornar a atividade do botnet cara para que o alvo não seja mais viável.



Geralmente, os bots são classificados como comuns ou direcionados:

- Bots comuns — Esses bots se identificam e não tentam emular navegadores. Muitos desses bots realizam tarefas úteis, como rastreamento de conteúdo, otimização de mecanismos de pesquisa

(SEO) ou agregação. É importante identificar e entender quais desses bots comuns chegam ao seu site e o efeito que eles têm no seu tráfego e desempenho.

- Bots direcionados — Esses bots tentam evitar a detecção emulando navegadores. Eles usam tecnologia de navegador, como navegadores sem cabeça, ou falsificam impressões digitais do navegador. Eles têm a capacidade de executar JavaScript e oferecer suporte a cookies. A intenção deles nem sempre é clara, e o tráfego que eles geram pode parecer tráfego normal de usuários.

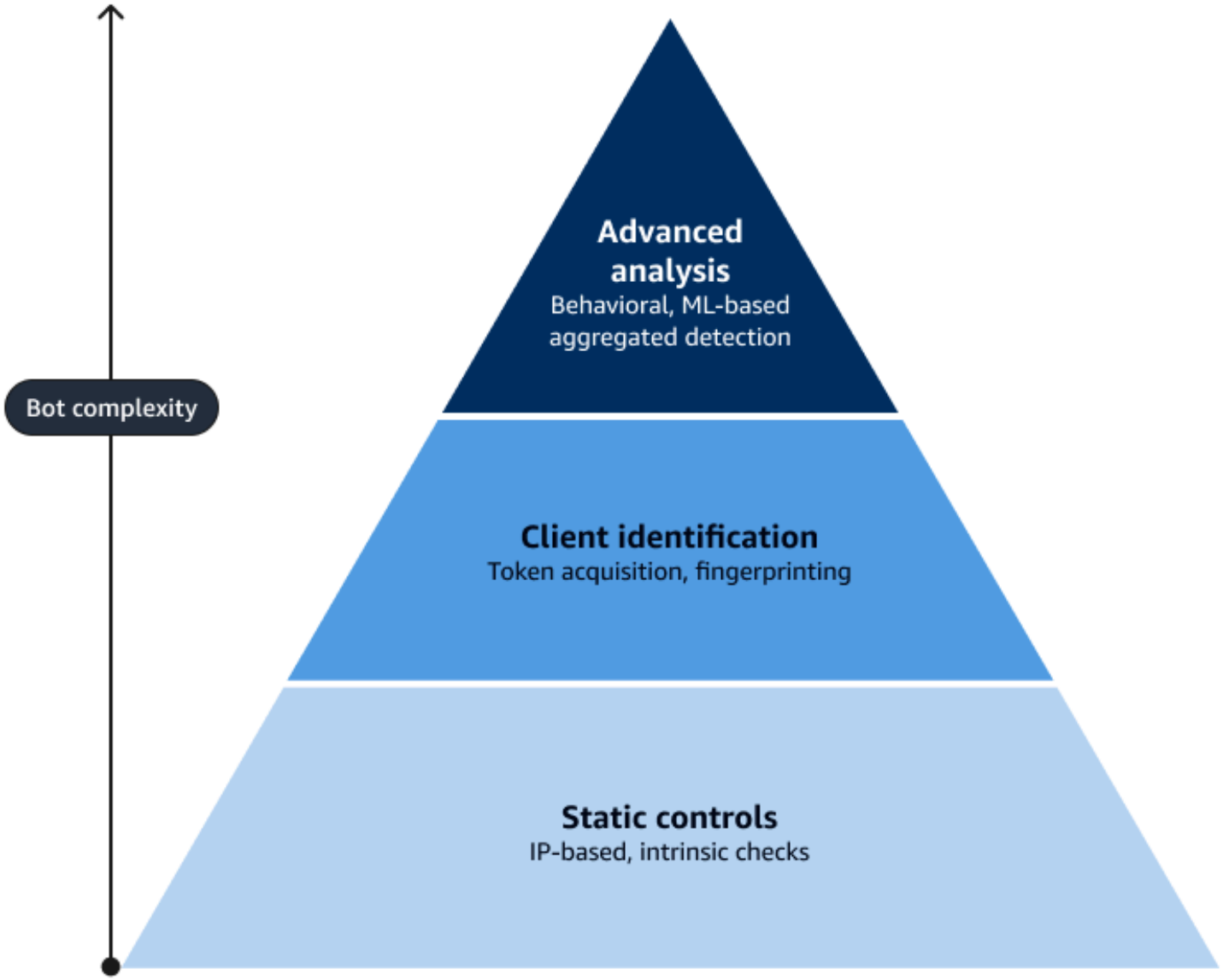
Os bots direcionados mais avançados e persistentes simulam o comportamento humano gerando movimentos e cliques de mouse semelhantes aos humanos em um site. Eles são os mais sofisticados e difíceis de detectar, mas também os mais caros de operar.

Muitas vezes, um operador combina essas técnicas. Isso cria um jogo de busca constante, em que você precisa alterar frequentemente a abordagem de proteção e mitigação para se adaptar às técnicas mais recentes do operador. Esses bots são considerados uma ameaça persistente avançada (APT). Para obter mais informações, consulte Ameaça persistente avançada no centro de recursos do NIST.

Técnicas para controle de bots

O principal objetivo da mitigação de bots é limitar o impacto negativo da atividade automatizada de bots nos sites, serviços e aplicativos de uma organização. A tecnologia e as técnicas usadas dependem do tipo de tráfego ou atividade contra a qual você deseja se defender. Compreender o aplicativo e seu tráfego é fundamental para fazer isso. Para obter mais informações sobre por onde começar, consulte a Diretrizes para monitorar sua estratégia de controle de bots seção deste guia.

Em geral, os controles que as soluções de mitigação de bots fornecem podem ser agrupados nas seguintes categorias de alto nível: estática, identificação do cliente e análise avançada. A figura a seguir mostra as diferentes técnicas disponíveis e como elas podem ser usadas dependendo da complexidade da atividade do bot. Isso destaca como a base, ou a mitigação mais ampla, pode ser obtida por meio do uso de controles estáticos, como listagem de permissões e verificações intrínsecas. A menor parte dos bots é sempre a mais avançada, e a mitigação desses bots requer tecnologia mais avançada e uma combinação de controles.



A seguir, este guia explora cada categoria e suas técnicas. Ele também descreve as opções disponíveis AWS WAFpara implementar esses controles:

- Controles estáticos para gerenciar bots
- Controles de identificação de clientes para gerenciar bots
- Controles avançados de análise para gerenciar bots

Controles estáticos para gerenciar bots

Para realizar uma ação, os controles estáticos avaliam as informações estáticas da solicitação HTTP (S), como o endereço IP ou os cabeçalhos. Esses controles podem ser úteis para atividades de bots

mal-intencionados de baixa sofisticação ou para o tráfego esperado de bots benéfico que precisa ser verificado e gerenciado. As técnicas de controle estático incluem: permitir listagem, controles baseados em IP e verificações intrínsecas.

Permitir listagem

Permitir listagem é um controle que permite identificar tráfego amigável por meio dos controles existentes de mitigação de bots. Há várias maneiras de fazer isso. O mais simples é usar uma regra que corresponda a um conjunto de endereços IP ou a uma condição de correspondência semelhante. Quando uma solicitação corresponde a uma regra definida como uma `Allow` ação, ela não é avaliada pelas regras subsequentes. Em alguns casos, você precisa evitar que apenas determinadas regras sejam aplicadas; em outras palavras, você precisa permitir uma lista para uma regra, mas não para todas as regras. Esse é um cenário comum para lidar com falsos positivos para regras. Permitir listagem é considerada uma regra de amplo escopo. Para reduzir o potencial de falsos negativos, recomendamos que você a combine com outra opção mais granular, como uma correspondência de caminho ou cabeçalho.

Controles baseados em IP

Blocos de endereço IP único

Uma ferramenta comumente usada para mitigar o impacto dos bots é limitar as solicitações de um único solicitante. O exemplo mais simples é bloquear o endereço IP de origem do tráfego se suas solicitações forem maliciosas ou tiverem alto volume. Isso usa regras de correspondência de conjuntos de AWS WAF IP para implementar blocos baseados em IP. Essas regras coincidem com os endereços IP e aplicam uma ação de `BlockChallenge`, ou`CAPTCHA`. Você pode determinar quando muitas solicitações estão chegando de um endereço IP examinando a Rede de Distribuição de Conteúdo (CDN), um firewall de aplicativo web ou registros de aplicativos e serviços. No entanto, na maioria dos casos, esse controle é impraticável sem automação.

A automatização de listas de bloqueio de endereços IP geralmente AWS WAF é feita com regras baseadas em taxas. Para obter mais informações, consulte Regras com base em taxa neste guia. Você também pode implementar as automações de segurança para a AWS WAF solução. Essa solução atualiza automaticamente uma lista de endereços IP a serem bloqueados, e uma AWS WAF regra nega solicitações que correspondam a esses endereços IP.

Uma forma de reconhecer um ataque de bot é se várias solicitações do mesmo endereço IP se concentrarem em um pequeno número de páginas da web. Isso indica que o bot está cortando

preços ou tentando repetidamente logins que falham em uma alta porcentagem. Você pode criar automações que reconheçam imediatamente esse padrão. As automações bloqueiam o endereço IP, o que reduz a eficácia do ataque ao identificá-lo e mitigá-lo rapidamente. O bloqueio de endereços IP específicos é menos eficaz quando um atacante tem uma grande coleção de endereços IP a partir dos quais lançar ataques ou quando o comportamento do ataque é difícil de reconhecer e separar do tráfego normal.

Reputação do endereço IP

Um serviço de reputação de IP fornece inteligência que ajuda a avaliar a confiabilidade de um endereço IP. Essa inteligência geralmente é derivada da agregação de informações relacionadas ao IP de atividades passadas desse endereço IP. A atividade anterior ajuda a indicar a probabilidade de um endereço IP gerar solicitações maliciosas. Os dados são adicionados às listas gerenciadas que rastreiam o comportamento do endereço IP.

Endereços IP anônimos são um caso especializado de reputação de endereços IP. O endereço IP de origem se origina de fontes conhecidas de endereços IP facilmente adquiridos, como máquinas virtuais baseadas em nuvem, ou de proxies, como provedores de VPN conhecidos ou nós Tor. Os grupos de regras gerenciados da AWS WAF Amazon IP Reputation List e Anonymous IP List usam a inteligência interna de ameaças da Amazon para ajudar a identificar esses endereços IP.

A inteligência fornecida por essas listas gerenciadas pode ajudá-lo a agir sobre as atividades identificadas a partir dessas fontes. Com base nessa inteligência, você pode criar regras que bloqueiam diretamente o tráfego ou regras que limitam o número de solicitações (como regras baseadas em taxas). Você também pode usar essa inteligência para avaliar a origem do tráfego usando as regras no `COUNT` modo. Isso examina os critérios de correspondência e aplica rótulos que você pode usar para criar regras personalizadas.

Regras com base em taxa

As regras baseadas em taxas podem ser uma ferramenta valiosa para determinados cenários. Por exemplo, as regras baseadas em taxas são eficazes quando o tráfego de bots atinge grandes volumes em comparação com usuários em identificadores uniformes de recursos (URIs) confidenciais ou quando o volume de tráfego começa a afetar as operações normais. A limitação de taxa pode manter as solicitações em níveis gerenciáveis e limitar e controlar o acesso. AWS WAF pode implementar uma regra de limitação de taxa em uma lista de controle de acesso à web (Web ACL) usando uma declaração de regra baseada em taxa. Uma abordagem recomendada ao usar regras baseadas em taxas é incluir uma regra geral que abranja todo o site, regras específicas de

URI e regras baseadas na taxa de reputação de IP. As regras baseadas na taxa de reputação de IP combinam a inteligência da reputação do endereço IP com a funcionalidade de limitação de taxa.

Para todo o site, uma regra geral baseada na taxa de reputação de IP cria um teto que impede que bots não sofisticados inundem um site a partir de um pequeno número de IPs. A limitação de taxa é especialmente recomendada para proteger URIs com alto custo ou impacto, como páginas de login ou criação de conta.

As regras de limitação de taxa podem fornecer uma primeira camada de defesa econômica. Você pode usar regras mais avançadas para proteger URIs confidenciais. As regras baseadas em taxas específicas do URI podem limitar o impacto em páginas críticas ou em APIs que afetam o back-end, como o acesso ao banco de dados. As mitigações avançadas para proteger determinados URIs, que serão discutidas posteriormente neste guia, geralmente incorrem em custos adicionais, e essas regras baseadas em taxas específicas de URI podem ajudá-lo a controlar os custos. Para obter mais informações sobre as regras baseadas em taxas comumente recomendadas, consulte As três regras baseadas em AWS WAF taxas mais importantes no Blog de Segurança. AWS Em algumas situações, é útil limitar o tipo de solicitação que é avaliada por uma regra baseada em taxas. Você pode usar instruções de escopo reduzido para, por exemplo, limitar as regras baseadas em taxas pela área geográfica do endereço IP de origem.

AWS WAF oferece um recurso avançado para regras baseadas em taxas por meio do uso de chaves de agregação. Com essa funcionalidade, você pode configurar uma regra baseada em taxa para usar várias outras chaves de agregação e combinações de chaves, além do endereço IP de origem. Por exemplo, como uma única combinação, você pode agregar solicitações com base em um endereço IP encaminhado, no método HTTP e em um argumento de consulta. Isso ajuda você a configurar regras mais refinadas para mitigação sofisticada de tráfego volumétrico.

Verificações intrínsecas

As verificações intrínsecas são vários tipos de validações ou verificações internas ou inerentes a um sistema ou processo. Para controle de bots, AWS WAF realiza uma verificação intrínseca validando se as informações enviadas na solicitação correspondem aos sinais do sistema. Por exemplo, ele realiza pesquisas reversas de DNS e outras verificações do sistema. Algumas solicitações automatizadas são necessárias, como solicitações relacionadas a SEO. Permitir a listagem é uma forma de permitir a entrada de bots bons e esperados. Mas, às vezes, bots maliciosos emulam bots bons, e pode ser difícil separá-los. AWS WAF fornece métodos para fazer isso por meio do grupo de regras gerenciado do AWS WAF Bot Control. As regras desse grupo fornecem a verificação de que os bots autoidentificados são quem dizem ser. AWS WAF verifica os detalhes da solicitação

em relação ao padrão conhecido desse bot e também realiza pesquisas reversas de DNS e outras verificações objetivas.

Controles de identificação de clientes para gerenciar bots

Se o tráfego relacionado ao ataque não puder ser facilmente reconhecido por meio de atributos estáticos, a detecção precisará ser capaz de identificar com precisão o cliente que está fazendo a solicitação. Por exemplo, as regras baseadas em taxas geralmente são mais eficazes e difíceis de evitar quando o atributo com limite de taxa é específico do aplicativo, como um cookie ou token. O uso de um cookie vinculado a uma sessão impede que os operadores de botnets possam duplicar fluxos de solicitações semelhantes em muitos bots.

A aquisição de tokens é comumente usada para identificação de clientes. Para aquisição de tokens, um JavaScript código coleta informações para gerar um token que é avaliado no lado do servidor. A avaliação pode variar desde a verificação do que JavaScript está sendo executado no cliente até a coleta de informações do dispositivo para impressão digital. A aquisição do token requer a integração de um JavaScript SDK ao site ou aplicativo, ou exige que um provedor de serviços faça a injeção dinamicamente.

Exigir JavaScript suporte adiciona um obstáculo adicional para os bots que tentam emular navegadores. Quando um SDK está envolvido, como em um aplicativo móvel, a aquisição de tokens verifica a implementação do SDK e impede que os bots imitem as solicitações do aplicativo.

A aquisição de tokens requer o uso de SDKs implementados no lado do cliente da conexão. Os AWS WAF recursos a seguir fornecem um SDK JavaScript baseado em navegadores e um SDK baseado em aplicativos para dispositivos móveis: Controle de bots, controle de fraudes, prevenção de aquisição de contas (ATP) e controle de fraudes, prevenção de fraudes na criação de contas (ACFP).

As técnicas de identificação do cliente incluem CAPTCHA, perfil do navegador, impressão digital do dispositivo e impressão digital TLS.

CAPTCHA

O teste de Turing público totalmente automatizado para diferenciar computadores e humanos (CAPTCHA) é usado para distinguir entre visitantes robóticos e humanos e para evitar a captura de dados na web, o preenchimento de credenciais e o spam. Há uma variedade de implementações, mas elas geralmente envolvem um quebra-cabeça que um ser humano pode resolver. Os

CAPTCHAs oferecem uma camada adicional de defesa contra bots comuns e podem reduzir os falsos positivos na detecção de bots.

AWS WAF permite que as regras executem uma ação CAPTCHA contra solicitações da web que correspondam aos critérios de inspeção de uma regra. Essa ação é o resultado da avaliação das informações de identificação do cliente coletadas pelo serviço. AWS WAF as regras podem exigir que os desafios do CAPTCHA sejam resolvidos para recursos específicos que são frequentemente alvos de bots, como login, pesquisa e envio de formulários. AWS WAF pode servir CAPTCHA diretamente por meios intersticiais ou usando um SDK para lidar com isso no lado do cliente. Para obter mais informações, consulte CAPTCHA e Challenge in. AWS WAF

Criação de perfil do navegador

O perfil do navegador é um método de coletar e avaliar as características do navegador, como parte da aquisição de tokens, para distinguir humanos reais usando um navegador interativo da atividade distribuída de bots. Você pode realizar a criação de perfil do navegador passivamente por meio de cabeçalhos, ordem dos cabeçalhos e outras características das solicitações que são inerentes ao funcionamento dos navegadores.

Você também pode realizar a criação de perfil do navegador no código usando a aquisição de tokens. Ao usar JavaScript o perfil do navegador, você pode determinar rapidamente se um cliente oferece suporte JavaScript. Isso ajuda você a detectar bots simples que não o suportam. O perfil do navegador verifica mais do que apenas cabeçalhos e JavaScript suporte HTTP; o perfil do navegador dificulta que os bots emulem totalmente um navegador da Web. As duas opções de perfil do navegador têm o mesmo objetivo: encontrar padrões em um perfil de navegador que indiquem inconsistência com o comportamento de um navegador real.

AWS WAF o controle de bots para bots direcionados fornece uma indicação, como parte da avaliação do token, de se um navegador mostra evidências de automação ou sinais inconsistentes. AWS WAF sinaliza a solicitação para realizar a ação especificada na regra. Para obter mais informações, consulte Detectar e bloquear tráfego avançado de bots no Blog AWS de segurança.

Impressão digital do dispositivo

A impressão digital do dispositivo é semelhante à criação de perfil do navegador, mas não se limita aos navegadores. O código executado em um dispositivo (que pode ser um dispositivo móvel ou um navegador da Web) coleta e reporta detalhes do dispositivo a um servidor de back-end. Os detalhes podem incluir atributos do sistema, como memória, tipo de CPU, tipo de kernel do sistema operacional (SO), versão do sistema operacional e virtualização.

Você pode usar a impressão digital do dispositivo para reconhecer se um bot está emulando um ambiente ou se há sinais diretos de que a automação está em uso. Além disso, a impressão digital do dispositivo também pode ser usada para reconhecer solicitações repetidas do mesmo dispositivo.

O reconhecimento de solicitações repetidas do mesmo dispositivo, mesmo que o dispositivo tente alterar algumas características da solicitação, permite que um sistema de back-end imponha regras de limitação de taxa. As regras de limitação de taxa baseadas na impressão digital do dispositivo geralmente são mais eficazes do que as regras de limitação de taxa baseadas em endereços IP. Isso ajuda você a reduzir o tráfego de bots que está alternando entre VPNs ou proxies, mas é proveniente de um pequeno número de dispositivos.

Quando usado com SDKs de integração de aplicativos, o controle de AWS WAF bots para bots direcionados pode agregar o comportamento da solicitação de sessão do cliente. Isso ajuda você a detectar e separar sessões de clientes legítimas de sessões de clientes mal-intencionados, mesmo quando ambas se originam do mesmo endereço IP. Para obter mais informações sobre o controle de AWS WAF bots para bots direcionados, consulte Detectar e bloquear tráfego avançado de bots no Blog AWS de segurança.

Impressão digital TLS

A impressão digital TLS, também conhecida como regras baseadas em assinatura, é comumente usada quando os bots se originam de muitos endereços IP, mas apresentam características semelhantes. Ao usar HTTPS, os lados do cliente e do servidor trocam mensagens para reconhecer e verificar um ao outro. Eles estabelecem algoritmos criptográficos e chaves de sessão. Isso é chamado de aperto de mão TLS. A forma como um handshake TLS é implementado é uma assinatura que geralmente é valiosa para reconhecer grandes ataques espalhados por vários endereços IP.

A impressão digital TLS permite que os servidores da Web determinem a identidade de um cliente da Web com um alto grau de precisão. Ele requer somente os parâmetros na primeira conexão de pacote, antes que qualquer troca de dados do aplicativo ocorra. Nesse caso, cliente web se refere ao aplicativo que inicia uma solicitação, que pode ser um navegador, uma ferramenta de CLI, um script (bot), um aplicativo nativo ou outro cliente.

Uma abordagem de impressão digital SSL e TLS é a impressão digital JA3. O JA3 imprime uma conexão de cliente com base nos campos da mensagem Client Hello do handshake SSL ou TLS. Ele ajuda você a criar perfis de clientes SSL e TLS específicos em diferentes endereços IP de origem, portas e certificados X.509.

A Amazon CloudFront suporta a adição de cabeçalhos JA3 às solicitações. Um `CloudFront-Viewer-JA3-Fingerprint` cabeçalho contém uma impressão digital de hash de 32 caracteres do pacote TLS Client Hello de uma solicitação recebida do visualizador. A impressão digital encapsula informações sobre como o cliente se comunica. Essas informações podem ser usadas para traçar o perfil de clientes que compartilham o mesmo padrão. Você pode adicionar o `CloudFront-Viewer-JA3-Fingerprint` cabeçalho a uma política de solicitação de origem e anexar a política a uma CloudFront distribuição. Em seguida, você pode inspecionar o valor do cabeçalho nos aplicativos de origem ou no Lambda @Edge CloudFront and Functions. Você pode comparar o valor do cabeçalho com uma lista de impressões digitais de malware conhecidas para bloquear os clientes mal-intencionados. Você também pode comparar o valor do cabeçalho com uma lista de impressões digitais esperadas para permitir solicitações somente de clientes conhecidos.

Controles avançados de análise para gerenciar bots

Alguns bots empregam ferramentas avançadas de engano para evitar ativamente a detecção. Esses bots imitam o comportamento humano para realizar uma atividade específica, como escalpelamento. Esses bots têm um propósito e geralmente estão vinculados a uma grande recompensa monetária.

Esses bots avançados e persistentes usam uma combinação de tecnologias para evitar a detecção ou se misturar ao tráfego normal. Por sua vez, isso também requer uma combinação de diferentes tecnologias de detecção para identificar e mitigar com precisão o tráfego malicioso.

Casos de uso direcionados

Os dados de casos de uso podem oferecer oportunidades de detecção de bots. As detecções de fraudes são casos de uso especiais em que uma mitigação especial é garantida. Por exemplo, para ajudar a evitar invasões de contas, você pode comparar uma lista de nomes de usuário e senhas de contas comprometidas com solicitações de login ou criação de conta. Isso ajuda os proprietários de sites a detectar tentativas de login que usam credenciais comprometidas. O uso de credenciais comprometidas pode indicar que bots estão tentando invadir uma conta, ou podem ser usuários que não sabem que suas credenciais estão comprometidas. Nesse caso de uso, os proprietários de sites podem tomar medidas adicionais para verificar o usuário e depois ajudá-lo a alterar a senha. AWS WAF fornece a regra gerenciada de prevenção de aquisição de contas (ATP) de controle de fraudes para esse caso de uso.

Detecção de bots agregados ou em nível de aplicativo

Alguns casos de uso exigem a combinação de dados sobre solicitações da rede de distribuição de conteúdo (CDN) e do back-end do aplicativo ou serviço. AWS WAFÀs vezes, você até precisa integrar inteligência de terceiros para poder tomar decisões de alta confiança sobre bots.

Funciona na Amazon CloudFront e AWS WAF pode enviar sinais para a infraestrutura de back-end ou, posteriormente, agregar regras por meio de cabeçalhos e rótulos. CloudFront expõe cabeçalhos de impressão digital JA3, conforme mencionado anteriormente. Este é um exemplo de CloudFront fornecimento desses dados por meio de um cabeçalho. AWS WAF pode enviar etiquetas quando corresponderem a uma regra. As regras subsequentes podem usar esses rótulos para tomar melhores decisões sobre bots. Quando várias regras são combinadas, você pode implementar controles altamente granulares. Um caso de uso comum é combinar partes de uma regra gerenciada por meio de um rótulo e depois combiná-la com outros dados de solicitação. Para obter mais informações, consulte Exemplos de correspondência de rótulos na AWS WAF documentação.

Análise de aprendizado de máquina

O aprendizado de máquina (ML) é uma técnica poderosa para lidar com bots. O ML pode se adaptar às mudanças nos detalhes e, quando combinado com outras ferramentas, fornece a maneira mais robusta e completa de mitigar bots com o mínimo de falsos positivos. As duas técnicas mais comuns de ML são análise comportamental e detecção de anomalias. Com a análise comportamental, um sistema (no cliente, no servidor ou em ambos) monitora como o usuário interage com o aplicativo ou site. Ele monitora os padrões de movimento do mouse ou a frequência das interações de clique e toque. O comportamento é então analisado com um modelo de ML para reconhecer bots. A detecção de anomalias é semelhante. Ele se concentra em detectar comportamentos ou padrões que são significativamente diferentes de uma linha de base definida para o aplicativo ou site.

AWS WAF controles direcionados para bots fornecem tecnologia de ML preditiva. Essa tecnologia ajuda a se defender contra ataques distribuídos baseados em proxy, feitos por bots projetados para evitar a detecção. O grupo gerenciado de regras de controle de AWS WAF bots usa análise automatizada de ML das estatísticas de tráfego do site para detectar comportamentos anômalos que são indicativos de atividades de bots distribuídas e coordenadas.

Implantação e implementação de sua estratégia de controle de bots

Há vários fatores a serem considerados ao planejar uma estratégia de implantação de controle de bots. Além das características exclusivas dos aplicativos web, o tamanho do ambiente, o processo de desenvolvimento e a estrutura organizacional afetam a estratégia de implantação. Dependendo das características do ambiente e do aplicativo, uma estratégia de implantação centralizada ou descentralizada pode ser usada:

- Estratégia de implantação centralizada — Uma abordagem centralizada permite um maior grau de controle quando você deseja uma aplicação rigorosa do controle de bots. Essa abordagem é adequada se as equipes de aplicativos preferirem aliviar o gerenciamento. Uma abordagem centralizada é mais eficaz quando os aplicativos da Web compartilham características semelhantes. Nesse caso, os aplicativos se beneficiam de um conjunto comum de regras de controle de bots e ações de mitigação de bots.
- Estratégia de implantação descentralizada — Uma abordagem descentralizada fornece às equipes de aplicativos autonomia para definir e implementar configurações de controle de bots de forma independente. Essa abordagem é comum em ambientes menores ou quando as equipes de aplicativos precisam manter o controle sobre suas políticas de controle de bots. Devido à natureza de muitos aplicativos da Web, geralmente é necessário manter políticas independentes de controle de bots, adaptadas às características exclusivas do aplicativo, resultando em uma abordagem descentralizada.
- Estratégia combinada — Uma combinação dessas duas abordagens é apropriada para uma combinação de aplicativos da web. Por exemplo, isso pode envolver um conjunto de regras básicas que se aplicam a todas as ACLs da web, enquanto o gerenciamento de políticas de controle de bots mais específicas é delegado às equipes de aplicativos.

Você pode usar AWS Firewall Managerpara centralizar e automatizar a implantação de ACLs da AWS WAF web que definem políticas de controle de bots. Ao usar o Firewall Manager, considere se é apropriado centralizar as políticas de controle de bots, inclusive se elas devem ser delegadas às equipes de aplicativos. Com o Firewall Manager, você pode usar a marcação para permitir que as equipes de aplicativos optem por AWS WAF políticas. Isso AWS WAF fornece uma funcionalidade inteligente de mitigação de ameaças. Você também pode ativar o AWS WAF registro centralizado para operações de aplicativos e segurança.

Independentemente da estratégia de implantação usada, é recomendável definir e gerenciar o processo de integração por meio de estruturas baseadas em infraestrutura como código (IaC), como AWS CloudFormationou o. AWS Cloud Development Kit (AWS CDK) Isso ajuda você a configurar o controle de origem para armazenar e configurar a versão dos objetos. Para obter mais informações, consulte exemplos de AWS WAF configuração para AWS CDK(GitHub) e CloudFormation(AWS documentação).

Estratégia de implementação

Depois de selecionar uma estratégia de implantação, a implementação pode começar. A estratégia de implantação define como as regras são implementadas em diferentes aplicativos. Na estratégia de implementação, o foco está no processo iterativo de adicionar controles, testar, monitorar continuamente e avaliar seus efeitos.

Entendendo os padrões de tráfego

Para realmente entender os padrões de tráfego, é importante se familiarizar com a função comercial e os atributos esperados do aplicativo, como padrões de uso, recursos essenciais e personas dos usuários. Incorpore o tráfego de produção e o tráfego gerado durante o teste no aplicativo para estabelecer uma linha de base para a avaliação. Certifique-se de que o cronograma inclua dados de tráfego que representem suficientemente vários picos de uso.

Usando sua ferramenta preferida, revise os registros e métricas de tráfego durante o período de uso representativo. Analise os dados de AWS WAF registro em busca de solicitações anômalas filtrando campos de registro como `headers` (por exemplo, `User-Agent` e`Referer`), e. `country` `clientIp` Anote os identificadores uniformes de recursos (URIs) e sua frequência de acesso. Categorize o tráfego, como identificar bons bots. Por exemplo, permita o acesso de bots benéficos, como rastreadores e monitores de mecanismos de pesquisa.

No AWS WAF console, no painel de controle de bots, uma amostra da atividade do bot está disponível para qualquer ACL da web ativa. Embora isso forneça uma perspectiva inicial dos volumes comuns de solicitações de bots, realize configurações e análises adicionais para entender melhor a atividade dos bots.

Para uma implementação eficaz, você deve ter uma boa compreensão do tráfego de bots, seus efeitos e quais solicitações de bots são benéficas versus maliciosas. Isso ajuda na próxima fase, selecionando controles, e ajuda você a avaliar o tráfego de bots em paralelo.

Seleção e adição de controles

A análise inicial do tráfego ajuda a determinar quais controles de bot usar e quais ações selecionar para cada um. Você também pode optar por registrar e monitorar atividades para possíveis ações futuras. A análise inicial do tráfego ajuda você a selecionar o melhor controle para gerenciar o tráfego. Para obter mais informações sobre os controles disponíveis, consulte Técnicas para controle de bots este guia.

Considere incluir implementações adicionais de SDK durante essa etapa. Isso ajuda você a testar e concluir as implementações do SDK em todos os aplicativos necessários. AWS WAF as regras de controle de bots e controle de fraudes fornecem um benefício completo de avaliação de tokens quando você implementa o JavaScript SDK ou o SDK móvel. Para obter mais informações, consulte Por que você deve usar os SDKs de integração de aplicativos com o Bot Control na AWS WAF documentação.

Recomendamos implementar a aquisição de tokens para diferentes tipos de aplicativos da seguinte forma:

- Aplicativo de página única (SPA) — JavaScript SDK (sem redirecionamento)
- Navegador móvel — JavaScript SDK ou ações de regras (CAPTCHA ou Desafio)
- Visualizações da Web — JavaScript SDK ou ações de regras (CAPTCHA ou Desafio)
- Aplicativos nativos — SDK móvel
- iFrames — SDK JavaScript

Para obter mais informações sobre como implementar os SDKs, consulte a integração AWS WAF do aplicativo cliente na AWS WAF documentação.

Teste e implantação na produção

Os controles devem ser implantados inicialmente em um ambiente que não seja de produção, onde você possa realizar testes para verificar se a funcionalidade esperada do aplicativo Web está preservada. Sempre realize uma validação completa em um ambiente de teste antes da implantação na produção.

Após o teste e a validação em um ambiente que não seja de produção, a versão de produção pode continuar. Selecione uma data e hora com o menor tráfego de usuários esperado. Antes da implantação, as equipes de aplicativos e segurança devem analisar a prontidão operacional, discutir

como reverter as alterações e revisar os painéis para garantir que todas as métricas e alarmes necessários estejam configurados.

Com a implantação CloudFront contínua da Amazon, você pode enviar uma pequena quantidade de tráfego para uma distribuição temporária que tenha uma ACL AWS WAF da web configurada especificamente para avaliação do controle de bots. AWS WAF fornece gerenciamento de versões de qualquer regra gerenciada nova ou atualizada para que você possa testar e aprovar as alterações antes que elas comecem a avaliar o tráfego de produção.

Avaliação e ajuste de controles

Os controles implementados podem fornecer mais informações e visibilidade sobre a atividade e os padrões de tráfego. Monitore e analise com frequência o tráfego de aplicativos para adicionar ou ajustar os controles de segurança. Normalmente, há uma fase de ajuste para mitigar possíveis falsos negativos e falsos positivos. Falsos negativos são ataques que não foram detectados por seus controles e exigem que você endureça suas regras. Os falsos positivos representam solicitações legítimas que foram identificadas incorretamente como ataques e bloqueadas como consequência.

A análise e o ajuste podem ser feitos manualmente ou com a ajuda de ferramentas. Um sistema de gerenciamento de eventos e informações de segurança (SIEM) é uma ferramenta comum que ajuda a fornecer métricas e monitoramento inteligente. Há muitos disponíveis com vários graus de sofisticação, mas todos fornecem um bom ponto de partida para obter informações sobre o tráfego.

Definir indicadores-chave de desempenho (KPIs) importantes para sites e aplicativos pode ajudá-lo a identificar mais rapidamente quando as coisas não estão funcionando conforme o esperado. Por exemplo, você pode usar cobranças de cartão de crédito, vendas por conta ou taxas de conversão como indicadores de anomalias comerciais que podem ser geradas por bots. Definir e entender quais métricas e KPIs são valiosos para monitorar é ainda mais importante do que apenas o ato de monitorar.

Entender como obter as métricas e os registros corretos de uma solução de controle de bots é tão importante quanto identificar as métricas a serem monitoradas. A próxima seção,Diretrizes para monitorar sua estratégia de controle de bots, detalha as opções de monitoramento e visibilidade a serem consideradas.

Diretrizes para monitorar sua estratégia de controle de bots

Para tráfego de bots e tráfego de aplicativos da web, o monitoramento e a visibilidade são de grande importância. Ele ajuda você a priorizar atividades e operações de segurança. Se o registro detalhado ou o uso de um sistema SIEM não forem possíveis, um bom ponto de partida é monitorar as métricas básicas fornecidas pela solução ou pelo fornecedor selecionado.

Essa visibilidade é útil para inteligência de ameaças, fortalecimento de regras, solução de falsos positivos e resposta a um incidente. Há várias opções de monitoramento disponíveis com AWS WAF. Para monitoramento de alto nível, AWS WAF fornece informações gerais do tráfego no AWS Management Console. Isso está disponível para todo o tráfego, bem como para uma visualização detalhada do tráfego de bots, quando o grupo de regras de controle de bots está ativado em sua ACL da web.

AWS WAF fornece opções diferentes para registro detalhado do tráfego de ACL da web. Você também pode adicionar rótulos às solicitações, que podem ser usados para facilitar a análise de registros e configurar as regras de avaliação de bots. Ao integrar o Amazon CloudWatch Logs Insights, você pode consultar os AWS WAF registros e visualizar os resultados.

Se você ativar o registro detalhado, AWS WAF fornece visibilidade adicional além do painel de controle de bots pré-configurado. O uso de AWS WAF registros para visualizar o tráfego, bem como investigações ad hoc, pode fornecer uma compreensão aprofundada dos padrões de tráfego e das opções de mitigação para um aplicativo web.

Você pode integrar dados de AWS WAF log com o Amazon CloudWatch Logs, o Amazon Simple Storage Service (Amazon S3) ou o Amazon Data Firehose. Para obter mais informações, consulte Ativar o AWS WAF registro e enviar registros para o CloudWatch Amazon S3 ou o Amazon Data Firehose. Você também pode enviar registros para vários destinos para análise, inclusive para o Amazon OpenSearch Service ou uma AWS Marketplacesolução. Para obter mais informações, consulte Configurações de destino na documentação do Firehose. Se várias fontes de registro forem usadas, uma solução de registro centralizada é recomendada para correlacionar as fontes.

A seguir, este guia fornece recomendações sobre como começar a monitorar o tráfego de bots e obter visibilidade usando a Amazon CloudWatch.

Rastreando as principais regras

O rastreamento das regras mais usadas pode destacar tendências e atividades potencialmente anômalas. O aumento das taxas de uma regra específica pode indicar um potencial falso positivo ou uma atividade direcionada que você deve investigar. A regra mais comum para rastreamento seriaControles baseados em IP: regras de bloqueio geográfico (um pico aqui pode mostrar tráfego de países incomuns, que podem não ser bloqueados automaticamente) e. Regras com base em taxa Essas regras sempre teriam variações inerentes, mas uma anomalia no padrão de tráfego pode ser indicativa da atividade do bot. Leve isso em consideração se você estiver definindo manualmente os limites.

Rastreando os principais rótulos e namespaces

Ao usar CloudWatch métricas para rastrear os principais rótulos, você pode ver quais AWS WAF regras são invocadas com frequência. Isso ajuda a detectar anomalias, como um aumento na atividade do scraper, tráfego de fontes suspeitas ou tentativa de abuso da página de login do aplicativo ou da API.

Veja a seguir exemplos de rótulos que podem ser interessantes:

- `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`
- `awswaf:managed:aws:bot-control:bot:category:http_library`
- `awswaf:managed:aws:bot-control:bot:name:curl`
- `awswaf:managed:aws:atp:signal:credential_compromised`
- `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
- `awswaf:managed:token:rejected`

Veja a seguir exemplos de namespaces de rótulos que podem ser interessantes:

- `awswaf:managed:aws:bot-control:`
- `awswaf:managed:aws:atp:`
- `awswaf:managed:aws:anonymous-ip-list:`

Criação de expressões matemáticas

Na Amazon CloudWatch, você pode criar expressões matemáticas para qualquer uma ou todas as regras. Se você definir alertas em expressões matemáticas, você será notificado sobre anomalias nas taxas, não nas quantidades, de determinadas métricas. Essa é uma ferramenta importante para reduzir a fadiga do alerta.

Crie uma métrica personalizada baseada em uma expressão matemática. Veja as taxas relativas das regras, com base no número total de solicitações para um aplicativo. A seguir está uma expressão matemática comum:

```
[ruleX count * 100]/[All allowed requests + All blocked requests]
```

Essa expressão matemática fornece uma porcentagem para que você possa rastrear uma regra específica e visualizar sua tendência ao longo do tempo.

Usar a detecção de anomalias

O uso da detecção de CloudWatch anomalias em qualquer CloudWatch métrica pode fornecer alertas sobre tendências anormalmente baixas ou altas, sem configurar manualmente o limite real. Esses algoritmos analisam continuamente métricas de sistemas e aplicativos, determinam linhas de base normais e anomalias superficiais com o mínimo de intervenção do usuário. CloudWatch aplica algoritmos estatísticos e de ML em seu recurso de detecção de anomalias.

Usando CloudWatch métricas da Amazon

AWS WAF processa o tráfego e adiciona rótulos às solicitações que correspondem às regras definidas na ACL da web. Cada rótulo cria uma métrica em CloudWatch. Ao mesmo tempo, cada regra de ACL da web também cria métricas para cada uma de suas ações possíveis. Use essas métricas de rótulos e ações para obter uma compreensão de alto nível do tráfego de bots. Essa é uma abordagem econômica para visualizar tendências. Para obter mais informações, consulte Exibir métricas disponíveis e Representar gráficos de métricas na CloudWatch documentação.

CloudWatch fornece a opção de enviar dados para um coletor ou agregador de registros, seja uma solução de terceiros AWS service (Serviço da AWS) ou uma solução de terceiros. A ingestão de dados CloudWatch pode fornecer uma experiência de observabilidade de segurança mais consolidada, na qual você pode correlacionar dados de várias fontes. Isso pode ajudá-lo a investigar, visualizar ou configurar seus alertas e automações de segurança.

Criando um painel

Depois de identificar as métricas importantes a serem monitoradas, crie um painel que contenha as métricas mais relevantes. Exibi-los side-by-side sob um único painel de vidro pode fornecer visibilidade e controle adicionais.

É sempre preferível configurar alertas e regras de automação para valores métricos anômalos. Não confie em humanos para identificar anomalias olhando para um painel. No entanto, os painéis podem ser úteis para fins de investigação após o recebimento de um alerta.

Otimizando custos para sua estratégia de controle de bots

A natureza do tráfego na web é dinâmica. Isso significa que a tecnologia e os serviços usados para mitigar as ameaças podem variar e ser ajustados ao longo do tempo. Isso é fundamental quando se considera uma estratégia de controle de bots e os controles incluídos nela. A otimização ao longo do tempo é o principal princípio a ser lembrado e vem do pilar de otimização de custos do AWS Well-Architected Framework.

AWS WAF as ACLs da web podem ser dinâmicas, especialmente quando novos recursos são lançados ou você está tentando mitigar uma nova ameaça. Monitorar seus custos envolve entender as dimensões de custo do AWS WAF serviço e como cada uma afeta seu gasto final. O principal custo de condução é o número de solicitações avaliadas pelo serviço. Há cobranças adicionais se você usar os grupos de regras gerenciados de controle de bots e prevenção de aquisição de contas (ATP) ou se usar ações avançadas, como CAPTCHA ou desafio.

Como os controles de bots especializados têm um custo premium, a principal meta de otimização de custos é reduzir o número de solicitações inspecionadas por esses controles avançados. As técnicas aplicáveis incluem separar conteúdo de alto valor, aplicar primeiro medidas de baixo custo, definir o escopo da área de avaliação e combinar a proteção de bots com outros tipos de controles. As técnicas de monitoramento de custos fornecem visibilidade adicional em toda a sua organização.

Separando conteúdo dinâmico e estático

Uma técnica de redução de custos é isolar o conteúdo estático do aplicativo dinâmico. A maioria das solicitações para aplicativos web típicos são solicitações para objetos estáticos. Um método comum para reduzir a carga nos servidores de aplicativos é mover o conteúdo estático para sua própria URL, como `static.example.com`. Isso geralmente é obtido criando uma distribuição exclusiva de entrega de conteúdo com a configuração de cache otimizada para conteúdo estático. Essa técnica também pode ajudar a reduzir os custos de controle de bots se o conteúdo estático não for comumente direcionado ao site ou ao aplicativo. Separar o conteúdo estático do aplicativo dinâmico pode permitir uma aplicação mais precisa dos controles avançados de bots.

Aplicando primeiro as regras de menor custo

Outra técnica é aplicar regras básicas de baixo custo que filtram o tráfego indesejado antes de usar controles avançados, que são mais caros. Na prática, isso geralmente significa colocar as mitigações de controle de bots como uma última camada de defesa e usar os controles anteriores para filtrar o

tráfego indesejado. Essa abordagem de pirâmide foi discutida anteriormente Técnicas para controle de bots neste guia. O objetivo principal é usar essas opções de baixo custo para interromper o tráfego indesejado, o que reduz o número de solicitações processadas por técnicas avançadas de mitigação de alto custo.

Definindo o escopo da área de avaliação

AWS WAF as instruções scope-down fornecem uma técnica poderosa para reduzir o número de solicitações inspecionadas por regras avançadas. Se a separação do conteúdo estático em seu próprio URL não puder ser implementada, as instruções de escopo reduzido são outro método para filtrar solicitações que não exigem técnicas avançadas de mitigação. Isso pode ser feito definindo um caminho de aplicativo específico, um método HTTP (como POST) ou uma combinação similar.

Combinando a proteção contra bots com outros controles

Considerações adicionais de controle de custos devem ser analisadas ao proteger aplicativos contra várias ameaças, além do tráfego indesejado de bots. Por exemplo, a proteção contra ataques distribuídos de negação de serviço (DDoS) e contra a invasão de contas exige uma configuração adicional que pode afetar os custos. O Shield Advanced é recomendado para ajudar a proteger os aplicativos contra ataques de DDoS. Em particular, suas mitigações na camada de aplicação podem resolver automaticamente as inundações de solicitações, reduzindo assim o número de solicitações que podem ser processadas pelo grupo de regras do AWS WAF Bot Control ao colocar a regra à frente na ordem de avaliação. O Shield Advanced tem um benefício adicional; AWS WAF regras padrão gerenciadas e personalizadas não têm custo adicional para recursos protegidos pelo Shield Advanced. Observe que grupos inteligentes de regras de mitigação de ameaças, incluindo o Bot Control, incorrem em custos adicionais, mesmo para recursos protegidos pelo Shield Advanced.

Os aplicativos que exigem prevenção de invasão de contas podem usar o grupo de regras de prevenção de aquisição de contas (ATP) do Controle de AWS WAF Fraudes. O custo de inspeção por solicitação do grupo de regras ATP é maior do que o do grupo de regras do Bot Control. Esse custo mais alto torna fundamental aplicar o grupo de regras ATP com a maior precisão possível. Usar o grupo de regras do Bot Control em conjunto com o ATP pode ajudar a alcançar esse objetivo. O grupo de regras de controle de bots deve ser colocado à frente do ATP na ACL da web para filtrar solicitações de bots e reduzir o número de solicitações inspecionadas pelo ATP.

Para otimização contínua, a atividade mais significativa é monitorar CloudWatchas métricas associadas ao grupo de regras do Bot Control. Com o passar do tempo, a meta é reduzir o número

de solicitações avaliadas pelo grupo de regras de controle de bots para somente aquelas que visam os recursos que você precisa para se proteger contra atividades indesejadas de bots. A criação de CloudWatch painéis fornece visibilidade das métricas mais importantes para aplicativos, incluindo AWS WAF custos e uso.

Custos de monitoramento

AWS Cost Explorer é uma ferramenta que permite visualizar e analisar seus custos e seu uso. O Cost Explorer facilita a análise dos AWS custos, incluindo os AWS WAF custos incorridos. A ferramenta fornece informações de custo dos últimos 12 meses e prevê gastos futuros para os próximos 12 meses.

AWS A detecção de anomalias de custos é outra ferramenta de controle de gerenciamento de custos que pode ser útil para monitorar AWS WAF custos. Ele usa tecnologias avançadas de ML para identificar gastos anômalos e causas-raiz. Isso ajuda você a agir rapidamente ou receber alertas se houver um aumento inesperado no custo. Para receber um alerta quando um limite de custo específico for atingido, AWS Budgetspode fornecer essa funcionalidade de rastreamento e monitoramento.

Recursos

AWS documentação

- AWS WAF guia do desenvolvedor
- AWS Melhores práticas para resiliência de DDoS (AWS whitepapers)
- Diretrizes para implementação AWS WAF (AWS Documentos técnicos)

Outros AWS recursos

- Análise de AWS WAF registros no Amazon CloudWatch Logs (postagem AWS do blog)
- Implante um painel AWS WAF com o mínimo esforço (postagem AWS no blog)
- Automações de segurança para AWS WAF (Biblioteca de AWS soluções)
- As três regras AWS WAF baseadas em tarifas mais importantes (AWS postagem no blog)
- Visualize AWS WAF registros com um CloudWatch painel da Amazon (postagem AWS no blog)

Colaboradores

Autoria

- Diana Alvarado, arquiteta sênior de soluções, AWS
- Cameron Worrell, arquiteto corporativo, AWS
- Geary Scherer, arquiteto de soluções, AWS
- Tzoori Tamam, arquiteta principal de soluções, AWS

Analisando

- Jess Izen, engenheira sênior de desenvolvimento de software, AWS
- Kaustubh Phatak, gerente sênior de produtos, AWS
- Vikramaditya Bhatnagar, consultor sênior de segurança, AWS

Redação técnica

- Lilly AbouHarb, redatora técnica sênior, AWS

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	—	21 de fevereiro de 2024

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

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

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

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

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja a inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade (ACID)

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

controle de acesso por atributo (ABAC)

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

fonte de dados autorizada

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

Zona de disponibilidade

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

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

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

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

B

bot ruim

Um bot destinado a perturbar ou causar danos a indivíduos ou organizações.

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

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

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também endianness.

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

acesso em vidro quebrado

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços conteinerizados na AWS.

planejamento de continuidade de negócios (BCP)

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

C

CAF

Consulte Estrutura de adoção da AWS nuvem.

implantação canária

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

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja a integração e a entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

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

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

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

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação — Fazer investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma landing zone, definir um CCo E, estabelecer um modelo de operações)
- Migração: migrar aplicações individuais
- Reinvenção: otimizar produtos e serviços e inovar na nuvem

Esses estágios foram definidos por Stephen Orban na postagem do blog The Journey Toward Cloud-First & the Stages of Adoption no blog de estratégia Nuvem AWS empresarial. Para obter

informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

Um campo da IA que usa aprendizado de máquina para analisar e extrair informações de formatos visuais, como imagens e vídeos digitais. Por exemplo, a Amazon SageMaker AI fornece algoritmos de processamento de imagem para CV.

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

O processo de automatizar os estágios de origem, criação, teste, preparação e produção do processo de lançamento do software. CI/CD is commonly described as a pipeline. CI/CDpode ajudá-lo a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte Benefícios da entrega contínua. CD também pode significar implantação contínua. Para obter mais informações, consulte Entrega contínua versus implantação contínua.

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

desvio de dados

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

dados em trânsito

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

malha de dados

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

implantação

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

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Veja a linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja a recuperação de desastres.

detecção de deriva

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

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

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

intercâmbio eletrônico de dados (EDI)

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

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o endpoint do serviço.

serviço de endpoint

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

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

ambiente

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

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

epic

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

ERP

Veja o planejamento de recursos corporativos.

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a filial.

recursos

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

importância do recurso

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

transformação de recursos

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

solicitação rápida

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

FGAC

Veja o controle de acesso refinado.

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

FM

Veja o modelo da fundação.

modelo de fundação (FM)

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

G

IA generativa

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

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

imagem dourada

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

estratégia greenfield

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

barreira de proteção

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

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que usa um mecanismo de banco de dados diferente (por exemplo, Oracle para Amazon Aurora). A migração heterogênea geralmente faz parte de um esforço de redefinição da arquitetura, e converter

o esquema pode ser uma tarefa complexa. O AWS fornece o AWS SCT para ajudar nas conversões de esquemas.

alta disponibilidade (HA)

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

modernização de historiador

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

dados de retenção

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

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

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

eu

IaC

Veja a infraestrutura como código.

Política baseada em identidade

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

aplicação ociosa

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

IIoT

Veja a Internet das Coisas industrial.

infraestrutura imutável

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

VPC de entrada (admissão)

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

migração incremental

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

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

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

VPC de inspeção

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

Internet das Coisas (IoT)

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

interpretabilidade

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

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

informações sobre zonas de pouso, consulte Configurar um ambiente da AWS com várias contas seguro e escalável.

modelo de linguagem grande (LLM)

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em etiquetas.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também endianness.

LLM

Veja um modelo de linguagem grande.

ambientes inferiores

Veja o ambiente.

M

machine learning (ML)

Um tipo de inteligência artificial que usa algoritmos e técnicas para reconhecimento e aprendizado de padrões. O ML analisa e aprende com dados gravados, por exemplo, dados da

Internet das Coisas (IoT), para gerar um modelo estatístico baseado em padrões. Para obter mais informações, consulte Machine learning.

ramificação principal

Veja a filial.

malware

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

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

conta de membro

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

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens (MQTT)

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

microsserviço

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

arquitetura de microsserviços

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

Programa de Aceleração da Migração (MAP)

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

migração em escala

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

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações,

analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte discussão sobre fábricas de migração e o guia do Cloud Migration Factory neste conjunto de conteúdo.

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja o aprendizado de máquina.

modernização

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

avaliação de preparação para modernização

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

aplicações monolíticas (monólitos)

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

MAPA

Consulte Avaliação do portfólio de migração.

MQTT

Consulte Transporte de telemetria de enfileiramento de mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja o controle de acesso de origem.

CARVALHO

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

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

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

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

OPC-UA

Consulte Comunicação de processo aberto — Arquitetura unificada.

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

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (OT)

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

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

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

controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo do Amazon Simple Storage Service (Amazon S3). O OAC oferece suporte a todos os buckets

S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e solicitações dinâmicas ao bucket S3. `PUT` `DELETE`

Identidade do acesso de origem (OAI)

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

ORR

Veja a análise de prontidão operacional.

OT

Veja a tecnologia operacional.

VPC de saída (egresso)

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

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja as informações de identificação pessoal.

manual

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

PLC

Consulte controlador lógico programável.

AMEIXA

Veja o gerenciamento do ciclo de vida do produto.

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pressão de predicados

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

controle preventivo

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

principal (entidade principal)

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

privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja o ambiente.

controlador lógico programável (PLC)

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

encadeamento imediato

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

pseudonimização

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

publish/subscribe (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

Veja responsável, responsável, consultado, informado (RACI).

RAG

Consulte Geração Aumentada de Recuperação.

ransomware

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

Matriz RASCI

Veja responsável, responsável, consultado, informado (RACI).

RCAC

Veja o controle de acesso por linha e coluna.

réplica de leitura

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

rearquiteta

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

Região

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

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

Geração Aumentada de Recuperação (RAG)

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

alternância

O processo de atualizar periodicamente um segredo para dificultar o acesso das credenciais por um invasor.

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

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

S

SAML 2.0

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

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

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

segurança por design

Uma abordagem de engenharia de sistemas que leva em conta a segurança em todo o processo de desenvolvimento.

controle de segurança

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

fortalecimento da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme medida por um indicador de nível de serviço.

modelo de responsabilidade compartilhada

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

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

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

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

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

CUSPE

Veja um único ponto de falha.

esquema de estrelas

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

padrão strangler fig

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

sub-rede

Um intervalo de endereços IP na VPC. Cada sub-rede fica alocada em uma única zona de disponibilidade.

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

prompt do sistema

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o ambiente.

V

aspiração

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

controle de versões

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

emparelhamento da VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte Estrutura de qualificação AWS da carga de trabalho.

escreva uma vez, leia muitas (WORM)

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

Z

exploração de dia zero

Um ataque, geralmente malware, que tira proveito de uma vulnerabilidade de dia zero.

vulnerabilidade de dia zero

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

aviso zero-shot

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

eficácia da solicitação zero depende da complexidade da tarefa e da qualidade da solicitação. Veja também a solicitação de algumas fotos.

aplicação zumbi

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

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