Guia de log e monitoramento para proprietários de aplicações

AWS Orientação prescritiva

AWS Orientação prescritiva: Guia de log e monitoramento para proprietários de aplicações

Table of Contents

Guia de log e monitoramento para proprietários de aplicações

John Buckley, Amazon Web Services (AWS)

Janeiro de 2023 (histórico do documento)

Uma workload é um conjunto de códigos e recursos que agrega valor empresarial, como uma aplicação voltada para o cliente ou um processo de back-end. Uma workload pode consistir em um subconjunto de recursos em uma única Conta da AWS ou pode abranger várias Contas da AWS. Na nuvem, uma aplicação é um tipo de workload. Ela pode ser implantada exclusivamente no ambiente de nuvem ou também pode ser hospedada em hardware local on-premises. Muitas publicações se concentram no log e no monitoramento da infraestrutura de nuvem e se destinam a equipes de segurança. Este guia é voltado para proprietários de aplicações e se concentra em abordagens eficazes e eficientes para registrar e monitorar aplicações na Nuvem AWS.

Ele também ajuda a definir o log e o monitoramento em um nível apropriado para que você possa identificar e responder rapidamente a anomalias. Isso ajuda você a garantir que os logs da aplicação permitam a análise detalhada e a resolução de quaisquer problemas.

Embora o guia tenha sido escrito tendo em mente as implantações na Nuvem AWS, esses princípios podem ser usados em aplicações executadas on-premises ou em outra infraestrutura de provedor de nuvem.

Resultados de negócios direcionados

Após ler este guia, você deverá entender:

- Os tipos de eventos comumente registrados em log para aplicações
- Os atributos do evento (como quem, o quê e quando) que você deve considerar registrar
- Os tipos de dados que você deve considerar excluir dos registros, como dados que possam comprometer sua postura de segurança ou informações de identificação pessoal
- Como definir o log e o monitoramento em um nível apropriado para sua aplicação
- Quem deve ser capaz de gerenciar e acessar os logs da sua aplicação
- Os recursos e Serviços da AWS podem ser configurados para monitorar e registrar em log suas aplicações na Nuvem AWS

- Como usar os dados de log da aplicação e recursos e Serviços da AWS para fazer a triagem e diagnosticar problemas

Sobre logs e o monitoramento de aplicações

Logs, monitoramento, alertas e relatórios são processos de segurança diferentes que trabalham juntos para fornecer visibilidade da integridade e da performance da sua aplicação. É fundamental criar e manter um registro detalhado das ações e eventos da sua aplicação para que você possa monitorar, alertar e gerar relatórios com base na atividade registrada.

Log de aplicações é o processo de coletar os eventos gerados pelas aplicações e gravá-los em um ou mais arquivos de log. Esse histórico de eventos pode ajudar você a realizar análises de segurança e performance, rastrear alterações de recursos e solucionar problemas de aplicações.

Monitoramento de aplicações é o processo de avaliar a performance geral e a integridade da aplicação. Você deve ser capaz de monitorar constantemente o front-end e o back-end da aplicação. Como as aplicações hospedadas na nuvem são altamente distribuídas, as ferramentas de log e monitoramento podem ajudar a solucionar rapidamente problemas de performance ou identificar e corrigir ameaças à segurança em tempo real. Os dados de log são uma entrada crítica para o monitoramento.

Observabilidade é um processo semelhante ao monitoramento, mas introduz maneiras de medir o comportamento da aplicação usando parâmetros diferentes, além de permitir correlações complexas. Um exemplo é medir a taxa de sucesso de HTTP em um dia específico para um conjunto de usuários em uma região geográfica específica. Para obter mais informações, consulte Monitoramento e observabilidade (marketing da AWS).

Em última análise, o objetivo dos proprietários de aplicações é manter aplicações seguras e íntegras e proporcionar experiências de usuário positivas com essas aplicações. Ao implementar o registro e o monitoramento, suas equipes de desenvolvedores e operações podem planejar e solucionar problemas de aplicações com mais rapidez.

O nível de log e monitoramento necessário varia para cada aplicação. Os fatores que podem afetar os níveis de log e registro incluem políticas e procedimentos organizacionais, o nível de risco de segurança que a aplicação representa, a importância da aplicação para as operações comerciais e a sensibilidade dos dados gerenciados pela aplicação. Em geral, as aplicações públicas ou voltadas para o cliente exigem um nível mais alto de monitoramento e log do que aquelas usadas internamente na organização. Este guia inclui informações gerais e recomendações, e você deve personalizar sua abordagem com base nos requisitos da aplicação.

> **Note**
>
> Os padrões ou procedimentos em sua organização podem exigir atributos específicos de log e monitoramento. Um exemplo é passar permissões de usuário para um sistema de revisão de direitos corporativos. Certifique-se de que seu plano de log e monitoramento atenda aos requisitos de sua organização.

Log de aplicações na Nuvem AWS

Para registrar em log aplicações na Nuvem AWS, analise os tipos de eventos, os atributos do evento e as práticas recomendadas.

Esta seção inclui os seguintes tópicos:

Tipos de eventos

Uma das considerações mais importantes ao estabelecer uma estratégia de log de aplicações é decidir quais eventos e ações registrar. Embora os requisitos da sua organização e da aplicação possam afetar essa decisão, recomendamos sempre registrar o seguinte em log, caso sejam válidos para sua aplicação:

- Falhas de validação de entrada: exemplos incluem violações de protocolo, codificações inaceitáveis e nomes e valores de parâmetros inválidos.
- Falhas de validação de saída: exemplos incluem incompatibilidades no conjunto de registros do banco de dados e codificação de dados inválida.
- Sucessos e falhas na autenticação de identidade: registre atividades de autenticação, mas não nomes de usuário e senhas. Como os usuários podem digitar acidentalmente suas senhas em um campo de nome de usuário, recomendamos não registrar nomes de usuário. Isso pode expor as credenciais de forma não intencional e resultar em acessos indesejados. Implemente controles de segurança para todos os logs que contêm dados de autenticação.
- Falhas de autorização (controle de acesso): para sistemas de autorização relacionados, registre as tentativas de acesso malsucedidas. É possível monitorar esses dados de log em busca de padrões que possam indicar um ataque ou problemas com o sistema de autorização na aplicação.
- Falhas de gerenciamento de sessões: exemplos incluem a modificação de cookies ou tokens de sessão. As aplicações geralmente usam cookies ou tokens para gerenciar os estados dos usuários. Usuários mal-intencionados podem tentar modificar os valores dos cookies para obter acesso não autorizado. O log de tokens de sessão adulterados fornece uma maneira de detectar esse comportamento.

- Erros de aplicações e eventos do sistema: exemplos incluem erros de sintaxe e de tempo de execução, problemas de conectividade, problemas de performance, mensagens de erro de serviços de terceiros, erros do sistema de arquivos, detecção de vírus para upload de arquivos e alterações na configuração.
- Estado da aplicação: inicie ou interrompa a aplicação e seus recursos relacionados.
- Estado do log: iniciar, parar ou pausar o log.
- Uso de funcionalidades de alto risco: exemplos incluem alterações na conexão de rede, adição ou exclusão de usuários, alteração de privilégios, atribuição de usuários a tokens, adição ou exclusão de tokens, uso de privilégios administrativos do sistema, acesso por administradores de aplicações, todas as ações realizadas por usuários com privilégios administrativos, acesso a dados de titulares de cartões de pagamento, uso de chaves de criptografia de dados, alteração de chaves de criptografia, criação e exclusão de objetos no nível do sistema, envio de conteúdo gerado pelo usuário (especialmente uploads de arquivos) e importação e exportação de dados (incluindo relatórios).
- Aceitações legais e outras: exemplos incluem permissões para recursos de telefonia móvel, termos de uso, termos e condições, consentimento de uso de dados pessoais e permissões para receber comunicações de marketing.

Além dos atributos recomendados para sua aplicação, considere quais atributos adicionais podem fornecer dados úteis para monitoramento, alertas e relatórios. Os exemplos incluem:

- Falhas de sequenciamento
- Atributos que ajudam você a avaliar o comportamento do usuário que viola a política de uso aceitável da sua organização
- Alterações em dados
- Atributos necessários para cumprir padrões ou regulamentações, como prevenção de crimes financeiros, limitação da negociação de ações ou coleta de informações de saúde ou outras informações pessoais.
- Atributos que ajudam a identificar comportamentos suspeitos ou inesperados, como tentativas de realizar ações não autorizadas
- Alterações de configuração
- Alterações em arquivos de código de aplicações ou na memória

Atributos do evento

Cada entrada do log precisa incluir informações suficientemente detalhadas para monitoramento e análise. Você pode registrar dados completos do conteúdo, mas é mais eficiente registrar uma visão geral ou propriedades resumidas. Os logs da aplicação devem registraroquando, onde, quem, o quê e qual de cada evento. Suas propriedades serão diferentes dependendo da arquitetura, da classe da aplicação e do sistema ou dispositivo host.

Ao registrar carimbos de data e hora, use o Horário Universal Coordenado (UTC) e os formatos de data e hora reconhecidos internacionalmente na norma ISO 8601 (site da ISO).

> **Note**
>
> Considere usar um serviço de sincronização de hora em rede para ajudar a garantir registros de data e hora precisos. A Amazon fornece o Serviço de Sincronização Temporal da Amazon, que é usado por muitos Serviços da AWS, incluindo o Amazon Elastic Compute Cloud (Amazon EC2). Esse serviço utiliza uma frota de relógios atômicos de referência conectados por satélite em cada Região da AWS para fornecer leituras precisas da hora atual no padrão global de Horário Universal Coordenado (UTC) via Network Time Protocol (NTP). Para obter mais informações, consulte Mantendo a hora com o Serviço de Sincronização Temporal da Amazon (publicação no blog da AWS).

Os atributos de eventos a seguir são normalmente incluídos nos logs.

Categoria de atributo	Atributo do evento	Descrição
Quando	Data e hora de log	Registre a data e a hora em que o evento foi adicionado ao log.
	Data e hora atuais	Registre a data e a hora em que o evento ocorreu. Isso pode ser diferente do registro de log, como quando o log é atrasado porque a aplicação cliente está hospedada em um dispositivo remoto que está

		online periódica ou intermitentemente.
	Identificador de eventos	Registre um nome de usuário, número de conta ou outro atributo exclusivo que garanta que o evento sempre possa ser identificado.
Onde	Identificador da aplicação	Registre o nome e a versão da aplicação.
	Endereço da aplicação	Registre o cluster ou o nome do host, o endereço IPv4 ou IPv6 do servidor, o número da porta, a identidade da estação de trabalho e o identificador do dispositivo local.
	Serviço	Registre o nome do serviço e o protocolo.
	Geolocalização	Registre as localizações geográficas do usuário.
	Janela, formulário ou página	Registre o URL do ponto de entrada, o método HTTP de uma aplicação Web ou o nome da caixa de diálogo em que a ação foi realizada.
	Localização do código	Registre o nome do script ou do módulo.
Quem (usuário humano ou máquina)	Endereço de origem	Registre o identificador do dispositivo, endereço IP, ID da torre de celular ou radiofrequência (RF) ou número de telefone celular do usuário.

	Identidade do usuário	Se o usuário estiver autenticado ou for conhecido, registre o valor da chave primária da tabela do banco de dados, o nome do usuário ou o número da licença.
	Classificação de tipos de usuários	Registre o tipo de usuário, como público, autenticado, CMS, mecanismo de pesquisa, testador de penetração autorizado ou monitor de tempo de atividade. Para obter mais informações sobre monitores de tempo de atividade, consulte Precauções e exclusões neste guia.
	Solicitar cabeçalhos HTTP ou agente de usuário HTTP	(Somente aplicações Web) Registre as informações do cabeçalho da solicitação HTTP, incluindo a string do agente de usuário HTTP, pois esses valores afetam as informações enviadas pelo cliente ao servidor.
O que	Tipo de evento	Registre se o evento é informativo, um aviso ou um erro.
	Gravidade do evento	Classifique a gravidade do evento, como alta, média e baixa.

Sinalizador de evento de segurança	Se o registro contiver dados não relacionados a eventos de segurança, crie um sinalizador para eventos relacionados à segurança para ajudar a identificá-los.
Descrição do evento	(Opcional) Inclua uma breve descrição do evento.
Ação ou intenção	Registre a finalidade original da solicitação, como fazer login, atualizar o ID da sessão, sair ou atualizar um perfil.
Resposta do usuário ou da aplicação	Registre a resposta do usuário ou da aplicação ao evento, como um código de status, mensagens de texto personalizadas, interrupção da sessão ou alertas do administrador.
Status do resultado	Registre se a ação foi bem-sucedida, como sucesso, falha ou adiamento.
Motivo do resultado	Registre o motivo pelo qual o status ocorreu. Por exemplo, uma solicitação de login pode falhar porque o usuário não está autenticado no banco de dados.

	Detalhes estendidos	Registre todas as informaçõ es adicionais associadas ao evento, como rastreame nto de pilha, mensagens de erro do sistema, informações de depuração e o corpo da solicitação HTTP.
	Código de status da resposta HTTP	(Somente aplicações Web) Registre o código de status da resposta HTTP retornado ao usuário, como `200` ou `301`. Para obter mais informações, consulte Níveis de log neste guia.
Qual	Recursos afetados	Registre quais recursos foram utilizados.
	Objeto	Registre componentes afetados ou outros objetos, como uma conta de usuário, recurso de dados, arquivo, URL ou ID de sessão.
	Nome do recurso	Registre os nomes dos recursos afetados.
	Tags de recursos	Registre as tags atribuídas aos recursos afetados. Para obter mais informações sobre etiquetas, consulte Marcar recursos da AWS com tags (Referência geral da AWS).

Outros	Confiança analítica	Registre a confiança do serviço de registro na detecção de eventos, como atribuir uma classificação baixa, média ou alta ou um valor numérico.
	Classificações internas	Registre quaisquer classific ações internas de respeito a padrões ou conformidade.
	Classificações externas	Registre quaisquer classific ações externas de respeito a padrões e conformidade, como o Security Content Automation Protocol (SCAP) do NIST.

Práticas recomendadas de log

Níveis de log

Tenha cuidado para não registrar em log uma quantidade excessiva de dados. Os logs devem capturar dados úteis e acionáveis. O excesso de log pode afetar negativamente a performance e aumentar os custos de armazenamento e processamento dos logs. O excesso de log também pode resultar em problemas e eventos de segurança que não são detectados.

Registrar os códigos de status de resposta HTTP pode gerar uma quantidade significativa de dados de log, especialmente códigos de status de nível 200 (sucesso) e nível 300 (redirecionamento). Recomendamos considerar registrar somente códigos de status no nível 400 (erros do lado do cliente) e no nível 500 (erros do lado do servidor).

As estruturas de log de aplicações fornecem diferentes níveis de log, como informações, depuração ou erro. Para ambientes de desenvolvimento, talvez você queira usar logs detalhados, por exemplo, incluir informações e depuração para ajudar seus desenvolvedores. No entanto, recomendamos desativar os níveis de informações e depuração para ambientes de produção porque eles podem gerar dados de log excessivos.

Precauções e exclusões

- Certifique-se de que os dados que você está registrando sejam legalmente permitidos, especialmente nas jurisdições em que sua organização opera.
- Não exclua nenhum evento de usuários conhecidos (como outros sistemas internos), terceiros confiáveis, robôs de mecanismos de pesquisa, monitores de tempo de atividade ou de processos e outros sistemas de monitoramento remoto. No entanto, é possível incluir um sinalizador de classificação para cada um deles nos dados registrados. Considere que os arquivos de log gerados por sua aplicação podem ser usados por terceiros, como soluções de monitoramento de log de terceiros ou provedores de serviços externos, que não estão autorizados a visualizar dados confidenciais processados pela aplicação.
- Os atributos a seguir não devem ser registrados diretamente nos logs. Remova, mascare, higienize, aplique hash ou criptografe o seguinte:
  - Código-fonte da aplicação
  - Valores de identificação da sessão (considere substituí-los por um valor com hash se precisar rastrear eventos específicos da sessão)
  - Tokens de acesso
  - Dados sigilosos e algumas formas de informações de identificação pessoal (PII), como informações de saúde ou identificadores emitidos pelo governo
  - Autenticação com senha
  - Strings de conexão de banco de dados
  - Chaves de criptografia e outros segredos primários
  - Dados do titular de contas bancárias ou cartões de pagamento
  - Dados de uma classificação de segurança mais alta do que o sistema de log pode armazenar
  - Informações comerciais confidenciais
  - Informações cuja obtenção é ilegal nas jurisdições relevantes
  - Informações cuja obtenção foi negada ou não consentida explicitamente por um usuário
  - Informações cuja permissão para obtenção expirou

Tipos de dados especiais

Algumas vezes, os dados a seguir também podem ser registrados em logs. Embora eles possam ser útil para fins investigativos e de solução de problemas, também podem revelar informações

confidenciais sobre o sistema. Talvez seja necessário anonimizar, fazer hash ou criptografar esses tipos de dados antes que o evento seja gravado:

- Caminhos do arquivo
- Nomes e endereços de rede internos
- Dados pessoais não confidenciais, como nomes pessoais, números de telefone e endereços de e-mail

Use a anonimização de dados se a identidade real do indivíduo não for exigida no log ou se o risco for considerado muito grande.

Gerenciamento de acesso e alterações

- Usuários não administrativos não devem ser capazes de desativar o log de eventos, especialmente aqueles que são necessários para atender aos requisitos de conformidade.
- Somente usuários administrativos devem ser capazes de pausar ou interromper o log de serviços ou modificar configurações.
- Se o seu serviço de log tiver um recurso de validação da integridade do arquivo de log, habilite-o. Isso ajuda você a detectar modificações, exclusões ou falsificação de arquivos de log. Para obter mais informações sobre este recurso nos Serviços da AWS, consulte Uso do CloudTrail neste guia.
- As alterações no log devem ser intrínsecas das aplicações, como se fossem feitas automaticamente pela aplicação com base em um algoritmo aprovado, ou seguir um processo de gerenciamento de alterações aprovado, como quando você altera os dados de configuração ou modifica o código-fonte.

Serviços da AWS para log e monitoramento

Este guia tem como foco aplicações de log e monitoramento implantadas na Nuvem AWS. É possível usar Serviços da AWS para implementar seu plano de log e monitoramento ou para ampliar suas soluções atuais. Por exemplo, se estiver solucionando um problema com sua aplicação, você poderá:

- Fazer a triagem dos logs da aplicação com o recurso VPC Flow Logs na Amazon Virtual Private Cloud (Amazon VPC) e visualizar o tráfego de rede que corresponde ao problema.
- Usar o AWS CloudTrail para visualizar as chamadas de API que correspondem aos horários dos eventos do problema.
- Revisar os logs no Amazon CloudWatch Logs para verificar se há picos de CPU que correspondam aos horários do evento do problema.

É possível implantar os seguintes recursos e Serviços da AWS para registrar e monitorar a aplicação:

- A AWS CloudTrail ajuda você a auditar a governança, a conformidade e o risco operacional da sua Conta da AWSregistrando as ações realizadas por um usuário, um perfil ou um AWS service (Serviço da AWS). Para obter mais informações sobre como usar esse serviço para registrar ou monitorar eventos para sua aplicação, consulte CloudTrail neste guia.
- O Amazon CloudWatch ajuda você a analisar logs e, em tempo real, monitorar as métricas dos seus recursos e aplicações hospedadas na AWS. Também é possível usar o recurso ServiceLens para monitorar a integridade da aplicação ou usar o recurso Synthetics para criar canários que monitoram seus endpoints e APIs. Para obter mais informações sobre como usar esse serviço para monitorar sua aplicação, consulte CloudWatch neste guia.
- O Amazon CloudWatch Logs ajuda a centralizar os logs de todos os seus sistemas, aplicações e Serviços da AWS para que você possa monitorá-los e arquivá-los com segurança. Para obter mais informações sobre como usar esse serviço para registrar eventos para sua aplicação, consulte CloudWatch Logs neste guia.
- O recurso VPC Flow Logs do Amazon Virtual Private Cloud (Amazon VPC) capturam informações do tráfego de IP de entrada e saída das interfaces de rede em sua VPC. Para obter mais informações sobre como usar esse serviço para registrar eventos para sua aplicação, consulte Logs de fluxo da VPC neste guia.

- O AWS X-Ray coleta dados sobre solicitações atendidas por sua aplicação e ajuda você a visualizar, filtrar e obter insights sobre esses dados para identificar problemas e oportunidades de otimização. Para obter mais informações sobre como usar esse serviço para monitorar sua aplicação, consulte X-Ray neste guia.

Log e monitoramento de aplicações com o AWS CloudTrail

O AWS CloudTrail é um AWS service (Serviço da AWS) que ajuda você a habilitar a auditoria operacional e de risco, a governança e a conformidade da sua Conta da AWS. As ações realizadas por um usuário, um perfil ou um AWS service (Serviço da AWS) são registradas como eventos no CloudTrail. Os eventos podem incluir ações realizadas no AWS Management Console, AWS Command Line Interface (AWS CLI) e nos SDKs e APIs da AWS.

Uso do CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando uma atividade ocorre na sua Conta da AWS, essa atividade é registrada em um evento do CloudTrail. Você pode visualizar facilmente os eventos recentes no console do CloudTrail acessando o Histórico de eventos.

Para obter um registro contínuo das atividade e dos eventos em sua Conta da AWS, crie uma trilha. É possível criar trilhas para uma única Região da AWS ou para todas as regiões. As trilhas registram arquivos de log em cada região, e o CloudTrail pode entregar arquivos de log a um bucket único e consolidado do Amazon Simple Storage Service (Amazon S3).

Você pode configurar várias trilhas de maneiras diferentes para que elas processem e registrem somente os eventos que você especificar. Isso pode ser útil quando você deseja fazer a triagem de eventos que ocorrem em sua Conta da AWS com eventos que ocorrem em sua aplicação.

> **Note**
>
> O CloudTrail tem um recurso de validação que pode ser usado para determinar se um arquivo de log foi modificado, excluído ou permaneceu inalterado depois que o CloudTrail o entregou. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Desse modo, é computacionalmente impraticável modificar, excluir ou forjar arquivos de log do CloudTrail sem detectar tais ações. Você pode usar a AWS CLI para validar os arquivos no local em que o CloudTrail

os forneceu. Para obter mais informações sobre esse recurso e como habilitá-lo, consulte Validar a integridade do arquivo de log do CloudTrail (documentação do CloudTrail).

Casos de uso do CloudTrail

- Auxílio para conformidade: usar o CloudTrail pode ajudar você a cumprir as políticas internas e os padrões regulatórios ao fornecer um histórico de eventos em sua Conta da AWS.
- Análise de segurança: é possível realizar análises de segurança e detectar padrões de comportamento do usuário ingerindo arquivos de log do CloudTrail em soluções de gerenciamento e análise de logs, como CloudWatch Logs, Amazon EventBridge, Amazon Athena, Amazon OpenSearch Service ou outra solução de terceiros.
- Exfiltração de dados: detecte a exfiltração de dados coletando dados de atividades em objetos do Amazon S3 por meio de eventos de API em nível de objeto registrados no CloudTrail. Depois que os dados da atividade forem coletados, você poderá usar outros Serviços da AWS, como EventBridge eAWS Lambda, para acionar uma resposta automática.
- Solução de problemas operacionais: é possível solucionar problemas operacionais usando os arquivos de log do CloudTrail. Por exemplo, você pode identificar rapidamente as alterações mais recentes feitas nos recursos em seu ambiente, incluindo criação, modificação e exclusão de recursos da AWS.

Práticas recomendadas para o CloudTrail

- Ative o CloudTrail em todas as Regiões da AWS.
- Habilite a validação da integridade dos arquivos de log.
- Criptografe logs.
- Ingira arquivos de log do CloudTrail no CloudWatch Logs.
- Centralize os registros de todos os Contas da AWS e regiões.
- Aplique políticas de ciclo de vida aos buckets do S3 que contêm arquivos de log.
- Impeça que os usuários desativem o log no CloudTrail. Aplique a política de controle de serviços (SCP) a seguir no AWS Organizations. Este SCP define uma regra de negação explícita para as ações `StopLogging` e `DeleteTrail` em toda a organização.

```
{
```

```
"Version": "2012-10-17",
"Statement":
       [
                 { "Action":
                     [
                     "cloudtrail:StopLogging",
                     "cloudtrail:DeleteTrail"
                      ],
                      "Resource": "*",
                      "Effect": "Deny"
                  }
        ]
}
```

Log e monitoramento de aplicações com o Amazon CloudWatch

O Amazon CloudWatch monitora os recursos da AWS e as aplicações que você executa na AWS em tempo real. Você pode usar o CloudWatch para coletar e monitorar métricas, que são as variáveis que é possível medir para avaliar seus recursos e suas aplicações.

Usar o CloudWatch

O CloudWatch é essencialmente um repositório de métricas. Um AWS service (Serviço da AWS), como o Amazon EC2, coloca métricas no repositório e você então recupera as estatísticas com base nessas métricas. Se você colocar suas próprias métricas personalizadas no repositório, poderá recuperar as estatísticas sobre essas métricas. Para obter mais informações, consulte Usar métricas do CloudWatch (documentação do CloudWatch).

Você também pode configurar alarmes que iniciam ações automaticamente em seu nome. Um alarme observa uma única métrica por um período especificado e realiza uma ou mais ações especificadas com base no valor da métrica em relação a um limite especificado ao longo do tempo. Por exemplo, o alarme poderia enviar uma notificação para um tópico do Amazon Simple Notification Service (Amazon SNS). Você também pode adicionar alarmes aos painéis. Para obter mais informações, consulte Usar alarmes do CloudWatch (documentação do CloudWatch).

O console CloudWatch exibe automaticamente métricas sobre cada AWS service (Serviço da AWS) usado por você. É possível criar painéis adicionais personalizados para exibir métricas e alarmes para suas aplicações. Para obter mais informações, consulte Usar painéis do CloudWatch (documentação do CloudWatch).

O CloudWatch oferece suporte automático a funcionalidade entre regiões. Você não precisa seguir nenhum passo adicional para exibir métricas de Regiões da AWS diferentes em uma única conta no mesmo gráfico ou painel. É possível obter a funcionalidade entre contas implementando a observabilidade entre contas(documentação do CloudWatch).

Para obter mais informações e orientações detalhadas sobre o uso do CloudWatch para registrar e monitorar workloads na Nuvem AWS, consulte Projetar e implementar log e monitoramento com o Amazon CloudWatch (Recomendações da AWS).

Casos de uso do CloudWatch

- Monitoramento da integridade de aplicações: o CloudWatch ServiceLens melhora a observabilidade dos serviços e das aplicações permitindo integrar rastreamentos, métricas, logs, alarmes e outros recursos de informação de integridade de recursos em um só lugar. O ServiceLens integra o CloudWatch ao AWS X-Ray para fornecer uma visão completa das aplicações a fim de ajudar a localizar gargalos de performance e a identificar com mais eficiência os usuários afetados. Para obter mais informações, consulte Usar o ServiceLens para monitorar a integridade de aplicações (documentação do CloudWatch).
- Monitoramento do Synthetic: é possível usar o Amazon CloudWatch Synthetics para criar canários, scripts configuráveis que são executados de acordo com uma programação, para monitorar seus endpoints e APIs. Os canários seguem as mesmas rotas e executam as mesmas ações que um cliente, o que possibilita verificar continuamente a experiência do cliente, mesmo quando você não tem nenhum tráfego de cliente em suas aplicações. Os canários verificam a disponibilidade e a latência dos endpoints e podem armazenar dados de tempo de carregamento e capturas de tela da interface do usuário. Eles monitoram as APIs REST, os URLs e o conteúdo do site e podem verificar se há alterações não autorizadas de phishing, injeção de código e scripts entre sites. Para obter mais informações, consulte Usar monitoramento do Synthetic (documentação do CloudWatch).
- Monitoramento de usuários: com o CloudWatch RUM, você pode realizar o monitoramento real do usuário para coletar e visualizar dados do lado do cliente sobre a performance da aplicação Web. Os dados incluem tempos de carregamento de página, erros no lado do cliente e comportamento do usuário. Você pode usar os dados coletados para identificar e depurar rapidamente problemas de performance do lado do cliente. Para obter mais informações, consulte Usar o CloudWatch RUM (documentação do CloudWatch).
- Detecção de comportamento anômalo: quando você habilita a detecção de anomalias para uma métrica, o CloudWatch aplica algoritmos estatísticos e de machine learning. Esses algoritmos analisam continuamente métricas de sistemas e aplicações, determinam linhas de base normais

e apontam anomalias. Para obter mais informações, consulte Usar a detecção de anomalias do CloudWatch (documentação do CloudWatch).

- Validação de recursos e experimentos A/B: você pode usar o Amazon CloudWatch Evidently para validar novos recursos com segurança oferecendo a eles um percentual especificado dos seus usuários enquanto implementa o recurso. Você também pode realizar experimentos A/B para decidir sobre design de recursos com base em evidências e dados. Para obter mais informações, consulte Executar lançamentos e experimentos A/B com o CloudWatch Evidently.

Log e monitoramento de aplicações com o Amazon CloudWatch Logs

O Amazon CloudWatch Logs permite centralizar os logs de todos os sistemas, aplicações e Serviços da AWS que você usa em um único serviço altamente escalável. Você pode visualizá-los facilmente, pesquisá-los por códigos de erro ou padrões específicos, filtrá-los com base em campos específicos ou arquivá-los com segurança para análise futura. Veja todos os logs de eventos, não importa a origem, como um fluxo único e consistente de eventos ordenados cronologicamente. Você pode consultá-los e classificá-los, agrupá-los por campos específicos, criar cálculos personalizados e visualizar dados de log em painéis.

Usar o CloudWatch Logs

No CloudWatch Logs, os eventos de log são organizados em fluxos de logs e grupos de logs. Stream de log é uma sequência de eventos de log que compartilham a mesma origem. Mais especificamente, um stream de log geralmente representa a sequência de eventos que vem da instância da aplicação ou do recurso que está sendo monitorado. Os grupos de logs definem um ou mais fluxos de logs que compartilham as mesmas configurações de retenção, monitoramento e controle de acesso. Cada fluxo de logs deve pertencer a um grupo de logs. Para obter mais informações, consulte Trabalhar com grupos de logs e fluxos de logs (documentação do CloudWatch Logs).

Use o CloudWatch Logs Insights para pesquisar e analisar dados de log no Amazon CloudWatch Logs. Realize consultas para ajudar a responder de maneira mais rápida e eficiente a problemas operacionais. Se um problema ocorrer, use o CloudWatch Logs Insights para identificar causas em potencial e validar correções implantadas. Para obter mais informações, consulte Analisar logs de dados com o CloudWatch Logs Insights (documentação do CloudWatch Logs).

É possível pesquisar e filtrar os dados de log que entram no CloudWatch Logs criando um ou mais filtros de métrica. Os filtros de métrica definem os termos e os padrões a serem procurados nos dados de log à medida que são enviados ao CloudWatch Logs. O CloudWatch Logs usa esses filtros de métrica para transformar os dados de log em métricas numéricas do CloudWatch que podem ser usadas para criar um gráfico ou definir um alarme. Para obter mais informações, consulte Criar métricas de eventos de logs usando filtros (documentação do CloudWatch Logs).

Casos de uso do CloudWatch Logs

- Monitorar logs do CloudTrail: é possível criar alarmes no CloudWatch e receber notificações de uma determinada atividade de API, conforme capturada pelo CloudTrail, e usar a notificação para solucionar problemas. Para obter mais informações, consulte Enviar eventos do CloudTrail para o CloudWatch Logs(documentação do CloudTrail).
- Log de chamadas da API da AWS: se você usa solução de monitoramento de terceiros, é possível usar o CloudWatch Logs para registrar chamadas da API da AWS. Você configura o serviço de monitoramento de terceiros para avaliar esse log e as APIs em nível de aplicação.
- Configurar a retenção de logs: por padrão, os logs no CloudWatch Logs são mantidos indefinidamente e nunca expiram. Você pode ajustar a política de retenção para cada grupo de logs, mantendo a retenção indefinida ou escolhendo um período de retenção entre 10 anos e um dia.
- Arquivamento e armazenamento de logs: você pode usar o CloudWatch Logs para armazenar seus dados de log em um armazenamento altamente durável. O agente do CloudWatch Logs envia os de dados de log com e sem alternância para o serviço de log. Em seguida, você poderá acessar os dados de log brutos quando forem necessários.

Log e monitoramento de aplicações com o VPC Flow Logs

O VPC Flow Logs é um recurso do Amazon Virtual Private Cloud (Amazon VPC) que ajuda a capturar informações do tráfego de IP de entrada e saída das interfaces de rede em sua VPC.

Usar o VPC Flow Logs

É possível criar um log de fluxo para uma nuvem privada virtual (VPC), sub-rede ou interface de rede. Se você criar um log de fluxo para uma sub-rede ou VPC, toda interface de rede na sub-rede ou VPC será monitorada. Para obter mais informações, consulte Trabalhar com logs de fluxo (documentação da Amazon VPC).

Os dados do log de fluxo para uma interface de rede monitorada são registrados como registros de log de fluxo. Um registro de log de fluxo representa um fluxo de rede na VPC. Por padrão, cada registro captura um fluxo de tráfego IP que ocorre em intervalo de agregação. Cada registro é uma string com campos separados por espaços. Um registro inclui valores para os diferentes componentes do fluxo IP como, por exemplo, a origem, o destino e o protocolo. Ao criar um log de fluxo, é possível usar o formato padrão do registro de log de fluxo ou especificar um formato personalizado. Para obter mais informações, consulte Exemplos de registro em logs de fluxo (documentação da Amazon VPC).

Os logs de fluxo não capturam as seguintes informações:

- O tráfego gerado por instâncias quando elas entram em contato com o servidor de Sistema de Nomes de Domínio (DNS) da Amazon. Se você usar seu próprio servidor de DNS, todo tráfego para esse servidor de DNS será registrado.
- O tráfego gerado por uma instância Windows para ativação de licença do Amazon Windows.
- O tráfego para e proveniente de `254.169.254` para metadados de instância.
- O tráfego para e proveniente de `254.169.123` para o Amazon Time Sync Service.
- Tráfego do Protocolo de Configuração Dinâmica de Host (DHCP)
- Tráfego para o endereço IP reservado para o router padrão da VPC.
- Trafegue entre uma interface de rede do endpoint e uma interface de rede do Network Load Balancer.

Os dados do log de fluxo podem ser publicados em vários Serviços da AWS, inclusive no Amazon CloudWatch Logs. Depois de criar um log de fluxo, você poderá recuperar e visualizar os registros do log de fluxo no CloudWatch Logs no grupo de logs que configurou. Para obter mais informações, consulte Publicar logs de fluxo no CloudWatch Logs (documentação da Amazon VPC).

Os dados do log de fluxo são coletados fora do caminho do tráfego de rede e, portanto, não afetam a throughput nem a latência da rede. É possível criar ou excluir logs de fluxo sem qualquer risco de impacto na pérformance da rede.

Casos de uso do VPC Flow Logs

- Diagnosticar regras de grupo de segurança excessivamente restritivas
- Monitorar o tráfego que chega à instância da sua aplicação
- Determinar a direção do tráfego

Log e monitoramento de aplicações com o AWS X-Ray

O AWS X-Ray coleta dados sobre solicitações atendidas por sua aplicação e ajuda você a visualizar, filtrar e obter insights sobre esses dados para identificar problemas e oportunidades de otimização.

Usar o X-Ray

O AWS X-Ray recebe rastreamentos da aplicação e, se estiverem integrados ao X-Ray, dos Serviços da AWS usados por sua aplicação. O X-Ray coleta amostras e visualiza solicitações em um gráfico de serviços quando eles fluem pelos componentes da sua aplicação. O X-Ray gera identificadores de rastreamento para que você possa correlacionar uma solicitação quando ela flui por vários componentes, o que ajuda a visualizar a solicitação de ponta a ponta. É possível aprimorar ainda mais esse processo incluindo anotações e metadados para ajudar a pesquisar e identificar de forma exclusiva as características de uma solicitação.

Recomendamos que configurar cada servidor ou endpoint em sua aplicação com o X-Ray. O X-Ray é implementado no código da aplicação por meio de chamadas ao serviço X-Ray. O X-Ray também fornece AWS SDKs para vários idiomas, incluindo clientes instrumentados que enviam dados automaticamente para o X-Ray. Os X-Ray SDKs fornecem patches para bibliotecas comuns usadas para fazer chamadas para outros serviços (por exemplo, HTTP, MySQL, PostgreSQL ou MongoDB).

Para obter mais informações, consulte Rastreamento de aplicações com o AWS X-Ray (Recomendações da AWS).

Casos de uso do X-Ray

- Análise e depuração de aplicações: os dados de rastreamento podem ajudar você a depurar a aplicação fornecendo uma visão completa da solicitação para que você possa identificar gargalos e solucionar problemas. O mapa de serviços o X-Ray é uma ferramenta visual que ajuda a identificar onde os erros estão ocorrendo, conexões com alta latência ou rastros de solicitações malsucedidas.
- Análise de performance: o Console de análise é uma ferramenta interativa de interpretação de dados de rastreamento que permite entender rapidamente a performance da aplicação e dos serviços subjacentes. O console ajuda você a explorar, analisar e visualizar rastreamentos. Também é possível comparar conjuntos de traços com condições diferentes para fins de análise de causa-raiz.

Perguntas frequentes

Posso usar meu serviço de monitoramento atual?

O Amazon CloudWatch é um serviço de monitoramento e observabilidade criado para engenheiros de DevOps, desenvolvedores, engenheiros de confiabilidade do site (SREs), gerentes de TI e proprietários de aplicações. Ele fornece dados e insights práticos para monitorar aplicações, compreender alterações de performance em todo o sistema e reagir a essas alterações, otimizar a utilização de recursos e obter uma visualização unificada da integridade operacional. No entanto, se você tiver um serviço de monitoramento estabelecido, não precisará substituí-lo.

Como faço para impedir que os arquivos de log sejam adulterados?

É possível habilitar a validação de integridade de arquivos de log. É prática recomendada gerenciar e armazenar seus logs em uma Conta da AWS dedicada e restringir o acesso a essa conta. Para obter mais informações, consulte Uso do CloudTrail neste guia.

Preciso manter arquivos de log separados para cada aplicação?

Não, é possível consolidar os dados de log de várias aplicações no mesmo arquivo de log. No entanto, certifique-se de que um identificador exclusivo para cada aplicação seja registrado no fluxo de logs.

Recursos

Documentação da AWS

- Documentação do AWS CloudTrail
- Documentação do Nuvem AWSWatch
- Documentação do Nuvem AWSWatch Logs
- Documentação do Amazon VPC Flow Logs
- Documentação do AWS X-Ray
- Projetar e implementar log e monitoramento com o Amazon CloudWatch (Recomendações da AWS)

Marketing da AWS

- AWS CloudTrail
- Amazon CloudWatch
- Logs centralizados na AWS (soluções da AWS)
- Monitoramento e observabilidade (operações da Nuvem AWS)
- Como monitorar suas aplicações de forma eficaz (AWS Startups)

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	—	6 de janeiro de 2023

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Aurora Edição Compatível com 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) para Oracle na nuvem. AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migrar seu sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: migre seu banco de dados Oracle local para o Oracle em uma instância do EC2 na 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. Esse cenário de migração é específico do VMware Cloud on AWS, que oferece suporte à compatibilidade de máquinas virtuais (VM) e à portabilidade da carga de trabalho entre seu ambiente local e. AWSÉ possível usar as tecnologias VMware Cloud Foundation de seus datacenters on-premises ao migrar sua infraestrutura para o VMware

Cloud na AWS. Exemplo: realocar o hipervisor que hospeda seu banco de dados Oracle para o VMware Cloud on. AWS

- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.
- Retirar: desative ou remova aplicações que não são mais necessárias em seu ambiente de origem.

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

O processo de usar técnicas de machine learning para resolver problemas operacionais, reduzir incidentes operacionais e intervenção humana e aumentar a qualidade do serviço. Para obter

mais informações sobre como as AIOps são usadas na estratégia de migração para a AWS , consulte o guia de integração de operações.

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para 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.

Availability Zone (zona de disponibilidade)

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o site da AWS CAF e o whitepaper da AWS CAF.

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

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS Schema Conversion Tool ()AWS SCT. Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

B

bot ruim

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

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

acesso em vidro quebrado

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços 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 da 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 postagens do CCoE no blog AWS Cloud Enterprise Strategy.

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 a AWS nuvem:

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

Esses estágios foram definidos por Stephen Orban na postagem do blog The Journey Toward Cloud-First & the Stages of Adoption no blog AWS Cloud Enterprise Strategy. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

Um processo para identificar e categorizar os dados em sua rede com base em criticalidade e confidencialidade. É um componente crítico de qualquer estratégia de gerenciamento de riscos de

segurança cibernética, pois ajuda a determinar os controles adequados de proteção e retenção para os dados. A classificação de dados é um componente do pilar de segurança no AWS Well-Architected Framework. Para obter mais informações, consulte Classificação de dados.

desvio de dados

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

dados em trânsito

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

malha de dados

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta é chamada de administrador delegado para esse serviço Para obter mais informações e uma

lista de serviços compatíveis, consulte Serviços que funcionam com o AWS Organizations na documentação do AWS Organizations .

implantação

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

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

recuperação de desastres (DR)

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

DML

Consulte linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja a recuperação de desastres.

detecção de deriva

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

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

computação de borda

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

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o endpoint do serviço.

serviço de endpoint

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

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

environment (ambiente)

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

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

epic

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

ERP

Consulte planejamento de recursos corporativos.

análise exploratória de dados (EDA)

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

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

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a filial.

recursos

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

importância do recurso

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

transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo,

se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

FGAC

Veja o controle de acesso refinado.

controle de acesso refinado (FGAC)

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

migração flash-cut

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

G

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

estratégia greenfield

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

barreira de proteção

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

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

migração homogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que compartilha o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server para Amazon RDS

para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

dados quentes

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

hotfix

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

período de hipercuidados

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

I

IaC

Veja a infraestrutura como código.

Política baseada em identidade

Uma política 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 segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

migração incremental

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

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet das Coisas Industrial (IIoT)

O uso de sensores e dispositivos conectados à Internet nos setores industriais, como manufatura, energia, automotivo, saúde, ciências biológicas e agricultura. Para obter mais informações,

consulte Construir uma estratégia de transformação digital para a Internet das Coisas Industrial (IIoT).

VPC de inspeção

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

Internet das Coisas (IoT)

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

interpretabilidade

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

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

migração de grande porte

: Uma migração de 300 servidores ou mais.

LBAC

: Veja controle de acesso baseado em etiquetas.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

: Veja 7 Rs.

sistema little-endian

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

ambientes inferiores

: Veja o ambiente.

M

machine learning (ML)

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

ramificação principal

Veja a filial.

malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, 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-membro

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

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens (MQTT)

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

microsserviço

Um serviço pequeno e independente que se comunica por meio de APIs bem definidas e normalmente pertence a equipes pequenas e autônomas. Por exemplo, um sistema de seguradora pode incluir microsserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos 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 APIs leves. 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 o Amazon EC2 AWS com o Application Migration Service.

Avaliação de Portfólio para Migração (MPA)

Uma ferramenta on-line que fornece informações para validar o caso de negócios para a migração para a AWS nuvem. 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 a AWS nuvem. 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 Avaliar a preparação para modernização de aplicações na AWS Cloud.

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 necessária nos projetos de adoção da nuvem. Para obter mais informações, consulte o guia do OCM.

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

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

OU

Veja a análise de prontidão operacional.

NÃO

Veja a tecnologia operacional.

VPC de saída (egresso)

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

P

limite de permissões

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

informações de identificação pessoal (PII)

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

PII

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja o ambiente.

controlador lógico programável (PLC)

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

pseudonimização

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

publicar/assinar (pub/sub)

Um padrão que permite comunicações assíncronas entre 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).

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)

Período de tempo aceitável máximo desde o último ponto de recuperação de dados. 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 atraso máximo aceitável entre a interrupção e a restauração do serviço.

refatorar

Veja 7 Rs.

Região

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

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

rotação

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

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

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login AWS Management Console ou chamar as operações da AWS API sem que você precise criar um usuário no IAM para todos

em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte Sobre a federação baseada em SAML 2.0 na documentação do IAM.

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

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

controle de segurança

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

fortalecimento da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

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

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

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

CUSPE

Veja um único ponto de falha.

esquema de estrelas

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

padrão strangler fig

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

sub-rede

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

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o ambiente.

V

aspiração

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

controle de versões

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

emparelhamento de VPC

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

vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte o AWS Workload Qualification Framework.

escreva uma vez, leia muitas (WORM)

Um modelo de armazenamento que grava dados uma única vez e evita que os dados sejam excluídos ou modificados. Os usuários autorizados podem ler os dados quantas vezes forem

necessárias, mas não podem alterá-los. Essa infraestrutura de armazenamento de dados é considerada imutável.

Z

exploração de dia zero

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

vulnerabilidade de dia zero

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

aplicação zumbi

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

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