Auditoria de instâncias, objetos de banco de dados e logins do SQL Server no Amazon RDS e no Amazon EC2

Recomendações da AWS

Recomendações da AWS: Auditoria de instâncias, objetos de banco de dados e logins do SQL Server no Amazon RDS e no Amazon EC2

Table of Contents

Auditoria de instâncias, objetos de banco de dados e logins do SQL Server no Amazon RDS e no Amazon EC2

Ashish Srivastava, Bhavani Akundi e Sreenivas Nettem, Amazon Web Services (AWS)

Abril de 2023 (histórico do documento)

Este guia explica como implementar o processo de auditoria do SQL Server para o SQL Server no Amazon Elastic Compute Cloud (Amazon EC2) e no Amazon Relational Database Service (Amazon RDS) para instâncias de banco de dados do SQL Server.

A auditoria de banco de dados é um método de auditoria de TI para certificar que os dados organizacionais estão seguros. Ela envolve a avaliação de dados e o registro em log das principais operações comerciais críticas em bancos de dados.

A auditoria do banco de dados tornou-se obrigatória, especialmente quando os dados incluem informações de identificação pessoal (PII) e precisam seguir as diretrizes de segurança e conformidade. Algumas diretrizes envolvem tipos de dados e recomendações publicadas pelas políticas de governança de um país. Um processo de auditoria requer evidências, que podem ser extraídas dos registros do banco de dados. A auditoria ajuda a impedir o acesso não autorizado à conta dos dados. Ao monitorar o uso de dados, você pode investigar atividades falsas e tomar as medidas apropriadas. A auditoria do banco de dados para fins de confidencialidade, integridade e acessibilidade dos dados ajuda a garantir a proteção dos dados. Para evitar violações de dados, a prática recomendada é implementar a segurança e a auditoria do banco de dados.

A auditoria do SQL Server é um requisito para cumprir padrões de segurança, financeiros e de saúde, como ISO/IEC 27001, o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS), o BASEL III, o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, Governança da Informação (IG) e a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA).

Resultados de negócios desejados

As organizações implementam a auditoria de bancos de dados e do SQL Server por vários motivos, incluindo os seguintes:

- Os auditores precisam de dados significativos e de contexto para conformidade e auditoria. Os logs de auditoria de banco de dados são adequados para equipes de DBA, mas não para auditores.
- A capacidade de gerar alertas críticos em caso de violação de segurança é um requisito básico para software de grande escala. Você pode usar logs de auditoria para essa finalidade, pois as informações de registro em log ajudam a identificar e rastrear as verificações de controle.
- A auditoria de banco de dados fornece informações como as seguintes:
  - Quem acessou os dados, por exemplo, DBAs, desenvolvedores, auditores, processos de extração, transformação e carregamento (ETL) e engenheiros de DevOps?
  - Qual era o estado anterior dos dados?
  - Quando os dados foram atualizados, o que foi modificado e por quê?
  - Uma pessoa autorizada aprovou a solicitação?
  - Os usuários internos estão usando seus privilégios adequadamente?
- Como as trilhas de auditoria ajudam na identificação de invasores, elas servem para impedir ações de agentes internos. Pessoas que sabem que suas ações são monitoradas têm menos probabilidade de acessar bancos de dados não autorizados ou de adulterar dados específicos.
- Finanças, medicina, energia, serviços de alimentação, obras públicas e muitos outros setores precisam analisar o acesso aos dados e produzir relatórios detalhados regularmente para agências governamentais. Por exemplo, os regulamentos da HIPAA exigem que os profissionais de saúde forneçam trilhas de auditoria que detalhem quem acessou os dados em seus registros, até o nível da linha e do registro. O RGPD tem requisitos semelhantes. A Lei Sarbanes Oxley (SOX) impõe uma ampla gama de regulamentações contábeis às empresas públicas. Essas organizações precisam analisar o acesso aos dados e produzir relatórios detalhados regularmente.

Visão geral dos níveis e processos de auditoria do SQL Server

As seções a seguir fornecem informações sobre auditoria em nível de servidor e banco de dados, processos de auditoria, benefícios e desvantagens.

Níveis de auditoria

A auditoria pode ser realizada no nível do SQL Server, no nível do banco de dados (o que envolve registrar em log os eventos associados às ações) ou nos dois níveis.

Auditoria em nível de servidor

Você pode usar o objeto de auditoria do SQL Server para auditar e coletar ações a monitorar. Você pode especificar uma única instância de ações e grupos de ações no nível do servidor. Você também pode criar várias auditorias para cada instância do SQL Server.

A auditoria no nível do SQL Server envolve parâmetros de configuração no nível do servidor, como xp_cmdshell e memória máxima do servidor. Para obter mais informações sobre configurações de memória de servidor, consulte a documentação do Microsoft SQL Server.

Auditoria em nível de banco de dados

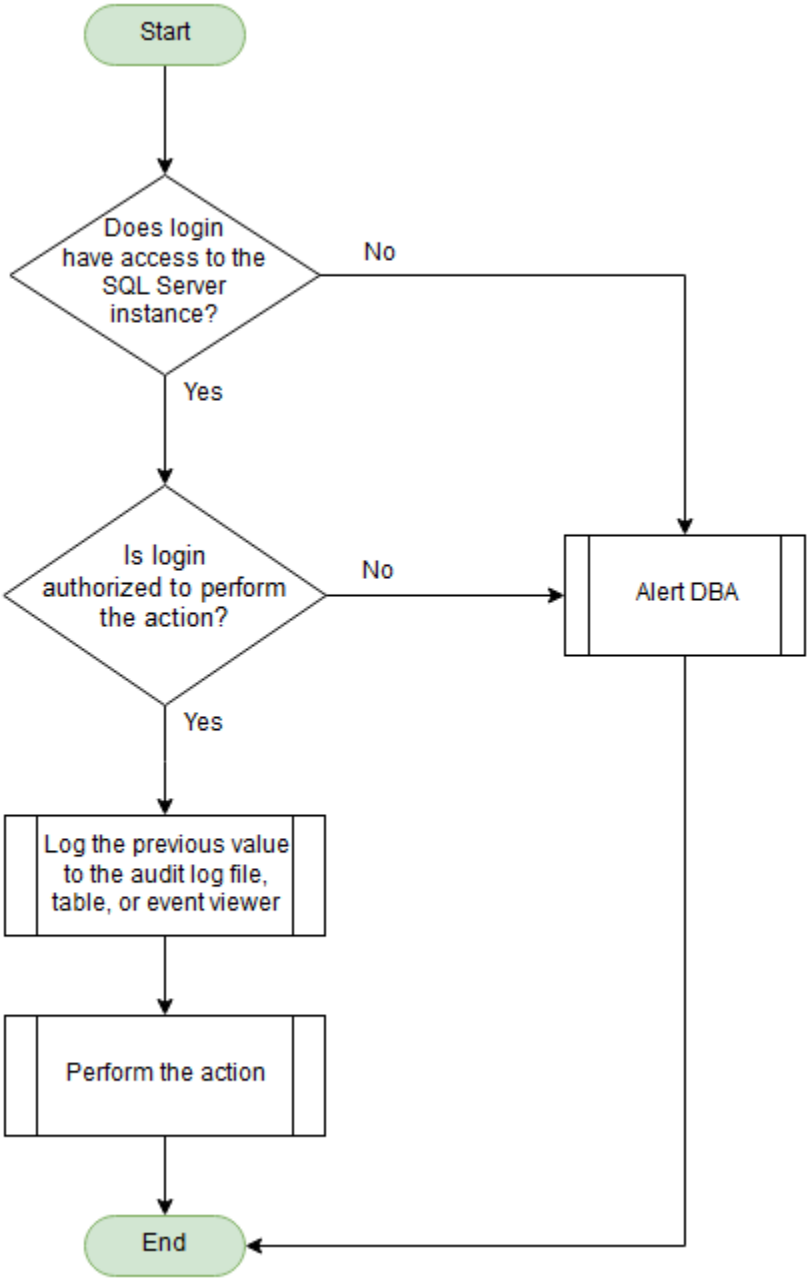
A auditoria em nível de banco de dados envolve a captura das ações dos usuários do banco de dados para fins de segurança. Por exemplo, você pode usar a auditoria em nível de banco de dados para garantir que usuários e processos não autorizados não possam acessar o banco de dados, e para verificar se as regras são aplicadas para restringir quaisquer atividades não autorizadas. Exemplos de auditoria em nível de banco de dados incluem a captura de todas as operações `INSERT`, `UPDATE`, `DELETE` e `TRIGGERS` no banco de dados.

Este guia fornece instruções e exemplos dos dois níveis de auditoria.

Fluxograma

O fluxograma a seguir ilustra o processo de auditoria do SQL Server. Quando um usuário ou processo faz login no sistema de banco de dados, suas credenciais de login são validadas. Se o

login for válido, o processo de auditoria verificará a autorização. Se o usuário ou processo estiver autorizado a realizar a ação, ele poderá concluir a ação e os dados auditados serão registrados em log na tabela de auditoria do banco de dados.



Vantagens e desvantagens de auditorias

Vantagens

- Ajuda a reduzir incidentes de violação de segurança ou quaisquer outras ações que possam resultar na divulgação não autorizada de informações confidenciais.
- Ajuda a identificar falhas e vulnerabilidades de segurança, incluindo acesso ilícito aos recursos, dados ou operações do banco de dados.
- Fornece uma trilha de auditoria das atividades para que você possa verificar e rastrear todos os tipos de transações e processos e rastrear consultas para analisar a performance.
- Torna as organizações mais responsáveis, pois elas podem revisar as informações rastreadas de auditoria e fornecer feedback para atender às metas de segurança e aos objetivos de performance.

Desvantagens

- Em geral, o impacto na performance é mínimo. No entanto, se a auditoria envolver um alto volume de rastreamento de transações, ela pode exigir recursos adicionais.
- Pode gerar muitos relatórios e documentos a serem visualizados e pode exigir o fornecimento de feedback paravárias equipes de gerenciamento e segurança.
- O consumo de recursos de armazenamento para armazenar os arquivos de auditoria pode ser alto.
- É necessária uma manutenção adicional para arquivar ou eliminar dados de auditoria antigos ou para mover tabelas para diferentes grupos de arquivos de banco de dados ou armazenamento.

Auditoria das instâncias de banco de dados do Amazon RDS para SQL Server

Esta seção fornece informações sobre as opções de auditoria do SQL Server no Amazon RDS, incluindo a criação de auditorias, a visualização de registros de auditoria e o monitoramento de resultados.

Pré-requisitos

- Um bucket do Amazon Simple Storage Service (Amazon S3) para armazenar os arquivos de auditoria
- Um perfil do AWS Identity and Access Management (IAM) para acessar o bucket do S3
- Um login de banco de dados com a permissão `ALTER ANY SERVER AUDIT` ou `CONTROL SERVER`

Versões compatíveis

- Para o Amazon RDS para SQL Server 2014, todas as edições são compatíveis com auditorias em nível de servidor. A edição Enterprise também é compatível com auditorias em nível de banco de dados.
- Começando com o SQL Server 2016 (13.x) SP1, todas as edições oferecem suporte a auditorias em nível de servidor e em banco de dados.
- O Amazon RDS é compatível com a auditoria do SQL Server em todas as Regiões da AWS, exceto Oriente Médio (Bahrein). Para obter as informações mais recentes, consulte Suporte para auditoria do SQL Server na documentação do Amazon RDS.

Uso do modo de auditoria C2

O modo de auditoria C2 é um parâmetro no grupo de parâmetros do banco de dados do Amazon RDS para SQL Server. O recurso é desabilitado por padrão. Você pode habiltá-lo atualizando o valor do parâmetro para 1. Quando o modo de auditoria C2 está habilitado, ele audita eventos como logins de usuários, chamadas de procedimentos armazenados e criação e exclusão de objetos. Esse modo pode gerar muitos dados porque audita tudo ou nada.

> **Important**
>
> A Microsoft planeja remover o modo de auditoria C2 em uma versão futura do SQL Server. Recomendamos evitar usar esse recurso.

Criação e visualização de auditorias

É possível auditar bancos de dados do Amazon RDS para SQL Server usando mecanismos de auditoria internos do SQL Server que envolvem criar auditorias e especificações de auditoria.

- Os logs de auditoria são enviados para um bucket do S3 usando um perfil do IAM que tem as permissões necessárias para acessar o bucket.
- Você pode escolher o perfil do IAM, o bucket do S3, a compactação e o período de retenção ao criar o grupo de opções. O período máximo de retenção é de 35 dias.
- Você cria o grupo de opções e o anexa a uma instância de banco de dados nova ou existente do Amazon RDS para SQL Server. Seus logs de auditoria são armazenados em `D:\rdsdbdata\SQLAudit`.
- Depois que o SQL Server terminar de gravar em um arquivo de logs de auditoria, ou quando o arquivo atingir seu limite de tamanho, o Amazon RDS o carregará no seu bucket do S3.
- Se a retenção estiver habilitada, o Amazon RDS vai transferir o arquivo para a pasta de retenção em `D:\rdsdbdata\SQLAudit\transmitted`. Registros de auditoria são mantidos na instância de banco de dados até que o arquivo de log de auditoria seja carregado.
- Você também pode encontrar registros de auditoria consultando por `dbo.rds_fn_get_audit_file`.

Para instâncias multi-AZ, os objetos de especificação de auditoria do banco de dados são replicados para todos os nós. A auditoria de servidor e as especificações de auditoria de servidor não são replicadas em todos os nós, portanto você deve criá-las manualmente.

Configuração do grupo de opções

Siga estas etapas para configurar um grupo de opções para realizar uma auditoria do SQL Server em sua instância de banco de dados do Amazon RDS para SQL Server. Para obter instruções detalhadas, consulte Auditoria do SQL Server na documentação do Amazon RDS.

- Crie um grupo de opções.
- Adicione a opção SQLSERVER_AUDIT ao grupo de opções.
- Para o destino do S3, crie um novo bucket ou selecione um bucket existente para os logs de auditoria.
- Para o perfil do IAM, crie um novo perfil ou escolha um perfil existente com as políticas necessárias. Para obter mais informações, consulte Criar manualmente um perfil do IAM para a auditoria do SQL Server na documentação do IAM.
- Expanda Informações adicionais e selecione Habilitar compactação para compactar logs de auditoria (recomendado).
- Para manter os logs de auditoria da instância de banco de dados, selecione Habilitar retenção e especifique um período de retenção (até um máximo de 35 dias).
- Aplique o grupo de opções a uma instância de banco de dados nova ou existente do Amazon RDS para SQL Server.
  - Para uma nova instância de banco de dados, aplique o grupo de opções ao executar a instância.
  - Para uma instância de banco de dados existente, modifique a instância e anexe o grupo de opções.

Criar auditorias

Para criar uma auditoria de servidor, utilize o script a seguir. Esse script cria o arquivo de auditoria no caminho do arquivo que você especifica. Para verificar a sintaxe, os argumentos e os exemplos, consulte a documentação do Microsoft SQL Server. Para evitar erros, revise a lista de limitações indicadas na documentação do Amazon RDS.

```
--Creating the server audit
 use master
 GO
 CREATE SERVER AUDIT [Audit-<<servername>>]
 TO FILE  ( FILEPATH = N'D:\rdsdbdata\SQLAudit', MAXSIZE = 2 MB, RESERVE_DISK_SPACE =
 OFF)
 WITH ( QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
 GO
-- Enabling the server audit
 ALTER SERVER AUDIT [Audit-<<servername>>] WITH (STATE = ON) ;
 GO
```

Criar especificações de auditoria

Depois de criar uma auditoria de servidor, você pode registrar eventos em nível de servidor criando uma especificação de auditoria de servidor com o código a seguir. Essa especificação determina o que será verificado durante a auditoria do servidor. Para verificar a sintaxe, os argumentos e os exemplos, consulte a documentação do Microsoft SQL Server. A especificação a seguir audita ações de login com falha e rastreia a criação, a alteração e a exclusão de objetos do servidor. Para obter uma lista, consulte a documentação do Microsoft SQL Server.

```
--Creating server audit specification
 USE [master]
 GO
 CREATE SERVER AUDIT SPECIFICATION [Audit-Spec-<<servername>>]
 FOR SERVER AUDIT  [Audit-<<servername>>]
 ADD (FAILED_LOGIN_GROUP), ADD (SERVER_OBJECT_CHANGE_GROUP)
 GO
--Enables the audit
 ALTER SERVER AUDIT [Audit-<<servername>>]
 WITH (STATE = ON);
 GO
```

É possível utilizar o código a seguir para criar uma especificação de auditoria de banco de dados que registre eventos em nível de banco de dados. Este exemplo audita as ações `INSERT`. Para verificar a sintaxe, os argumentos e mais exemplos, consulte a documentação do Microsoft SQL Server.

```
--Creating database audit specification
 USE [<<DBName>>]
 GO

 CREATE DATABASE AUDIT SPECIFICATION [DatabaseAuditSpecification-<<DBName>>]
 FOR SERVER AUDIT [Audit-<<ServerName>>]
 ADD (INSERT ON DATABASE::[<<DBName>>] BY [dbo])
 WITH (STATE = ON)
 GO
```

Visualizar logs de auditoria

Use a consulta a seguir para visualizar logs de auditoria. Os logs de auditoria são mantidos na instância de banco de dados até serem enviados ao Amazon S3. Se você habilitar a retenção para

a opção SQLSERVER_AUDIT, o Amazon RDS moverá o arquivo para a pasta de retenção `D:\rdsdbdata\SQLAudit\transmitted`.

Você também pode visualizar registros de auditoria na sua pasta de retenção, alterando o filtro para `D:\rdsdbdata\SQLAudit\transmitted\*.sqlaudit`.

```
--Viewing audit logs
SELECT   *
 FROM     msdb.dbo.rds_fn_get_audit_file
             ('D:\rdsdbdata\SQLAudit\*.sqlaudit'
             , default
             , default )
--Viewing audit logs in retention folder
SELECT   *
 FROM     msdb.dbo.rds_fn_get_audit_file
             ('D:\rdsdbdata\SQLAudit\transmitted\*.sqlaudit'
             , default
             , default )
```

Opções adicionais para auditar bancos de dados do SQL Server são discutidas abaixo na documentação da AWS e da Microsoft:

- Eventos estendidos do SQL Server: consulte a publicação do Blog da AWS Set up Extended Events in Amazon RDS for SQL Server.
- Gatilhos do SQL Server: consulte Criar uma regra que é acionada em um evento do Amazon RDS na documentação do Amazon RDS.
- Rastreamento de alterações: consulte Track data changes na documentação do Microsoft SQL Server.
- Captura de dados de alteração: consulte Usar a captura de dados de alteração na documentação do Amazon RDS.
- Parâmetro do modo de auditoria C2: consulte a c2 audit mode Server Configuration Option na documentação do Microsoft SQL Server.

Monitoramento

Você pode usar os fluxos de atividades do banco de dados no Amazon RDS para integrar eventos de auditoria do SQL Server com ferramentas de monitoramento de atividades de bancos de dados da

Imperva, McAfee e IBM. Para obter mais informações, consulte a página Auditing in Microsoft SQL Server na documentação do Amazon RDS.

Auditoria do SQL Server em instâncias de bancos de dados do Amazon EC2 ou do Amazon RDS Custom

Esta seção fornece informações sobre as opções de auditoria do SQL Server no Amazon EC2 e no Amazon RDS Custom, incluindo a criação de auditorias de servidores e bancos de dados, a visualização de logs de auditoria e o monitoramento de resultados.

Pré-requisitos

- Login do banco de dados com a permissão `ALTER ANY SERVER AUDIT` ou `CONTROL SERVER`

Versões compatíveis

- Qualquer edição do SQL Server versão 2016 e posterior

Uso do modo de auditoria C2

O modo de auditoria C2 audita eventos como logins de usuários, chamadas de procedimentos armazenados e a criação e exclusão de objetos. Esse modo pode gerar muitos dados porque audita tudo ou nada. Os logs de auditoria C2 são armazenados no diretório de dados padrão da instância do SQL Server. Cada arquivo de logs tem um limite máximo de 200 MB. Um novo arquivo é criado automaticamente quando esse limite é atingido. Você pode habilitar a auditoria C2 com o uso do SQL Server Management Studio. Para obter mais informações, consulte a documentação do Microsoft SQL Server.

> **Important**
>
> A Microsoft planeja remover o modo de auditoria C2 em uma versão futura do SQL Server. Recomendamos evitar usar esse recurso.

Para usar o modo de auditoria C2 para auditar logins com falha:

1. No SQL Server Management Studio, conecte-se à instância do SQL Server para a qual você deseja habilitar a auditoria.

2. Selecione a instância do SQL Server, clique com o botão direito do mouse e escolha Propriedades e depois Segurança.
3. Em Auditoria de login, escolha uma opção de configuração. Você pode auditar somente logins com falha, somente logins com êxito, ambos ou nenhum. (O padrão é somente logins com falha.)
4. Em Opções, selecione Habilitar rastreamento de auditoria C2.

Criação e visualização de auditorias

Criação de auditorias de servidores

Uma auditoria de servidor no SQL Server coleta ações em nível de instância ou de banco de dados para monitorar. A saída de auditoria é salva em um caminho de arquivo de destino de auditoria, em um log de segurança do Windows ou em um log de aplicação.

Para criar uma auditoria de servidor:

1. No SQL Server Management Studio, no Explorador de Objetos, expanda Segurança, clique com o botão direito do mouse em Auditorias e escolha Nova Auditoria.Isso cria um novo objeto de auditoria do SQL Server para auditoria em nível de servidor.
2. Em Destino da auditoria, escolha um arquivo, um log de segurança ou um log de aplicação.
3. Se você selecionou um arquivo como destino, especifique a localização da pasta.
4. Configure outras opções e, em seguida, escolha OK.
5. Para habilitar a auditoria, clique com o botão direito do mouse na nova configuração de auditoria e escolha Habilitar auditoria.

Para obter mais informações, consulte a documentação do Microsoft SQL Server.

Criação de especificações de auditoria de servidor

A especificação de auditoria do servidor coleta muitos grupos de ação em nível de servidor criados pelo recurso SQL Server Extended Events. Você pode incluir grupos de ações de auditoria em uma especificação de auditoria do servidor. Essas ações são enviadas para a auditoria que as registra no arquivo ou log de destino.

Para criar uma especificação de auditoria de servidor:

1. No SQL Server Management Studio, no Explorador de Objetos, expanda Segurança, clique com o botão direito do mouse em Especificações de auditoria de servidor e escolha Nova especificação de auditoria de servidor.
2. Em Auditoria, escolha a auditoria de servidor que você criou anteriormente.
3. Em Ações, escolha o tipo de ação de auditoria que especifica os grupos de ações de auditoria no nível do servidor e as ações de auditoria que você deseja capturar e, em seguida, escolha OK.
4. Para habilitar a especificação de auditoria de servidor, clique com o botão direito do mouse na nova especificação e escolha Habilitar especificação de auditoria de servidor.

Para obter mais informações, consulte Create a Server Audit and Server Audit Specification e SQL Server Audit Action Groups and Actions na documentação do Microsoft SQL Server.

Criação de especificações de auditoria de banco de dados

Você pode criar um objeto de especificação de auditoria de banco de dados para auditoria em nível de banco de dados. Essa especificação define os grupos de ações de auditoria em nível de banco de dados e as ações de auditoria a serem capturadas.

Para criar uma especificação de auditoria de banco de dados:

1. No SQL Server Management Studio, no Explorador de Objetos, expanda o banco de dados que você deseja auditar.
2. Expanda a pasta Segurança, clique com o botão direito do mouse em Especificações de auditoria de banco de dados, e escolha Nova especificação de auditoria de banco de dados.
3. Em Ações, configure um ou mais tipos de ação de auditoria de banco de dados. Selecione as instruções que você deseja auditar (como DELETE ou INSERT) e a classe de objeto na qual realizar a ação.
4. Quando tiver concluído suas seleções, escolha OK.
5. Para habilitar a especificação de auditoria do banco de dados, clique com o botão direito do mouse na nova especificação e escolha Habilitar especificação de auditoria de banco de dados.

Para obter mais informações, consulte Create a server audit and database audit specification e SQL Server Audit Action Groups and Actions na documentação do Microsoft SQL Server.

Visualização de logs de auditoria do SQL Server

Para visualizar logs de auditoria:

1. No SQL Server Management Studio, clique com o botão direito do mouse no objeto de auditoria do SQL Server e escolha Visualizar logs de auditoria.

   O visualizador de arquivos de logs exibe o log de auditoria independentemente de sua localização (um arquivo ou o log de eventos do Windows).
2. Para personalizar as entradas de logs que são exibidas, escolha Filtrar.
3. Para exportar o log para um arquivo de logs, escolha Exportar.
4. Quando terminar de visualizar o log, escolha Fechar.

Para obter mais informações, consulte a documentação do Microsoft SQL Server.

Monitoramento

Você pode monitorar logs de auditoria registrados em um arquivo de auditoria, em uma aplicação ou um log de eventos de segurança ou em uma tabela de auditoria no banco de dados usando soluções de monitoramento como o Nagios. Uma solução de monitoramento integrada a um mecanismo de geração de tíquetes ou alertas pode gerar alertas e incidentes em tempo real para notificar o administrador do sistema ou do banco de dados.

Requisitos de armazenamento e computação para auditoria

Para o Amazon RDS

- Os logs de auditoria são primeiro armazenados localmente em disco no local `D:\rdsdbdata\SQLAudit`. Em seguida, o Amazon RDS carrega esses arquivos em um bucket do S3 que é configurado no grupo de opções `SQLSERVER_AUDIT` usando o perfil do IAM especificado.
- Se a retenção estiver habilitada, o Amazon RDS vai transferir o arquivo para a pasta de retenção em `D:\rdsdbdata\SQLAudit\transmitted`. Registros de auditoria são mantidos na instância de banco de dados até que o arquivo de logs de auditoria seja carregado no Amazon S3.
- Certifique-se de provisionar espaço de armazenamento suficiente para a instância com base no período de retenção.
- O consumo de CPU para executar auditorias geralmente é mínimo. Monitore o uso da CPU ao executar consultas de auditoria e dimensione a instância de banco de dados Amazon RDS de acordo. Você pode monitorar as métricas do Amazon RDS com o Amazon CloudWatch.

Para o Amazon EC2

- Verifique se há espaço de armazenamento suficiente provisionado na unidade que armazena os arquivos de logs de auditoria com base no período de retenção.
- O consumo de CPU para executar auditorias geralmente é mínimo. Monitore o uso da CPU ao executar consultas de auditoria e dimensione a instância do EC2 de acordo. Você pode usar o Amazon CloudWatch para monitorar instâncias do EC2.

Práticas recomendadas para auditar o SQL Server na AWS

Ao auditar bancos de dados do SQL Server na AWS, siga estas práticas recomendadas.

- Entenda os requisitos de auditoria. Verifique se a solução de auditoria precisa atender aos requisitos de conformidade, como RGPD ou HIPAA. Por exemplo, a solução de auditoria pode precisar rastrear e registrar em log todas as alterações realizadas em dados críticos, como PII e informações financeiras.
- Defina o escopo da auditoria. Decida se você precisa auditar todas as instâncias do SQL Server ou somente instâncias específicas que hospedam bancos de dados críticos. No nível do banco de dados, determine se você precisa auditar todas as tabelas ou somente as tabelas que contêm dados críticos.
- Identifique a lista de eventos que você deseja rastrear e registrar em log. Por exemplo, sua lista de auditoria pode incluir falhas de login, alterações na permissão de login, novos logins e usuários e logins e usuários excluídos.
- Escolha a ferramenta certa de auditoria. Por exemplo, se você quiser auditar somente eventos de login e logout, você pode usar logs de erros ou eventos estendidos. Se quiser auditar alterações na linguagem de manipulação de dados (DML), use captura de dados de alteração (CDC), rastreamento de alterações ou tabelas temporais. Se você quiser auditar as alterações no nível da instância e do banco de dados, use o recurso de auditoria do SQL Server. Ou você pode usar uma ferramenta de auditoria de terceiros, como ApexSQL Audit.
- Configure alertas em tempo real para notificar proativamente os DBAs ou a equipe de segurança quando uma ação específica não atender aos requisitos de conformidade.
- Revise os dados de auditoria periodicamente criando um painel simples ou um relatório que leia os dados de auditoria e filtre as ações nas quais você está interessado.
- Configure um alerta para monitorar as alterações realizadas na solução de auditoria.
- Defina políticas de retenção para os dados de auditoria com base nos requisitos da sua empresa, e arquive os dados de auditoria antigos.

Perguntas frequentes

Esta seção fornece respostas para as perguntas frequentes sobre auditoria de instâncias do SQL Server no Amazon RDS e no Amazon EC2.

Quais são os principais componentes do recurso de auditoria do SQL Server?

O recurso de auditoria do SQL Server tem três componentes principais:

- Os objetos de auditoria do SQL Server definem o caminho para armazenar as informações de auditoria, o modo de sincronização de auditoria, o mecanismo de substituição do arquivo de auditoria e a ação a ser executada em caso de falhas de auditoria.
- As especificações de auditoria do servidor rastreiam e registram em log as alterações que são realizadas no nível da instância do SQL Server e os eventos gerados pelo recurso SQL Server Extended Events.
- As especificações de auditoria de banco de dados rastreiam e registram em log diferentes tipos de ações que são executadas no nível do banco de dados e eventos gerados pelo recurso SQL Server Extended Events.

Quais são alguns eventos críticos que eu devo considerar auditar?

Os eventos críticos incluem logins com falha, alterações de login, de usuário, de esquema e de auditoria.

Por que é importante auditar logins com falha e alterações de login e de usuários?

Por exemplo, tentativas excessivas de login malsucedidas ou alterações na permissão do usuário podem indicar que um ataque está em andamento.

Por que é importante auditar alterações de esquema?

Recomendamos que você acompanhe todas as alterações de esquema do banco de dados para detectar quaisquer alterações que não tenham sido autorizadas.

Por que é importante auditar o sistema de auditoria?

A auditoria das alterações em sua solução de auditoria do SQL Server ajuda você a identificar usuários não autorizados que possam estar tentando desabilitar o processo de auditoria para realizar atividades ilegais ou não compatíveis. Essa auditoria também ajuda você a atender aos requisitos do auditor quanto à integridade dos logs da solução de auditoria, fornecendo evidências que abrangem todos os cenários. Outro uso simples dessa auditoria é lembrar o administrador do banco de dados para reabilitar a auditoria caso ela tenha sido desabilitada para fins de manutenção.

Como posso usar gatilhos para auditar alterações no banco de dados?

Você pode criar gatilhos em tabelas que contêm dados críticos para registrar em log dados alterados ou inseridos e comparar os dados antes e depois da modificação. Você pode usar o gatilho `INSTEAD OF` para evitar alterações em uma tabela específica e registrar em log a ação que falhou.

Quais são as vantagens e desvantagens de usar a CDC para auditar alterações no banco de dados? Quais versões são compatíveis com a CDC?

A captura de dados de alteração (CDC) é compatível com todas as edições do SQL Server 2016 e posteriores. Nas versões anteriores, somente a edição Enterprise é compatível com a CDC.

Confira algumas das vantagens de usar a CDC para auditar alterações no banco de dados:

- Você pode usar a CDC como uma solução de auditoria assíncrona do SQL Server para rastrear operações de linguagem de manipulação de dados (DML) em tabelas.
- A CDC rastreia as operações `INSERT`, `UPDATE` e `DELETE` em tabelas de banco de dados e registra informações detalhadas sobre essas alterações em tabelas espelhadas.
- A CDC depende do log de transações do SQL Server como fonte de alterações nos dados.

- Você pode configurar facilmente a CDC usando os comandos Transact-SQL.

Desvantagens:

- A CDC não manipula automaticamente as alterações da linguagem de definição de dados (DDL) em tabelas habilitadas para CDC. Isso exige um esforço extra para refletir as alterações de DDL na tabela de rastreamento.
- A CDC não oferece nenhuma opção para rastrear a instrução `SELECT`.
- O SQL Server mantém os dados de rastreamento da CDC na tabela de alterações por apenas uma quantidade configurável de dias.
- Os trabalhos da CDC não funcionarão a menos que o serviço do agente do SQL Server esteja em execução.

Recursos

- Auditoria do SQL Server (documentação do Amazon RDS)
- How to enable auditing for Amazon RDS for SQL Server (workshop do Amazon RDS para SQL Server)
- Trabalhar com a notificação de eventos do Amazon RDS (documentação do Amazon RDS)
- Audit and accountability in Amazon EC2 (documentação do Amazon EC2)
- Migrating SQL Server databases to the Nuvem AWS (Recomendações da AWS)
- Best practices for deploying Microsoft SQL Server on Amazon EC2 (Recomendações da AWS)

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Publicação inicial	—	20 de abril de 2023

Glossário de Recomendações da AWS

Os termos a seguir são comumente usados em estratégias, guias e padrões fornecidos pelas Recomendações da AWS. 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 a edição do Amazon Aurora 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: migrar seu banco de dados Oracle on-premises 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: migrar seu banco de dados Oracle on-premises 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. Você migra servidores de uma plataforma on-premises para um serviço de nuvem para a mesma plataforma. Exemplo: migrar uma aplicação Microsoft Hyper-V para a 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

Veja controle de acesso baseado em atributo.

serviços abstraídos

Veja 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 em que 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 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 aplicações

Uma abordagem de segurança que permite o uso somente de aplicações aprovadas 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 para AWS na documentação do AWS Identity and Access Management (IAM).

fonte de dados autorizada

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

zona de disponibilidade

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

AWS Cloud Adoption Framework (AWS CAF)

Uma estrutura de diretrizes e práticas recomendadas da AWS para ajudar as organizações a desenvolverem um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS A 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. Para essa perspectiva, a 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 Workload Qualification Framework (AWS WQF)

Uma ferramenta que avalia os workloads de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS A WQF é fornecida com o 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 malicioso

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

BCP

Veja 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 da aplicação em um ambiente (azul) e a nova versão da aplicação no outro ambiente (verde). Essa estratégia ajuda você a reverter rapidamente com o mínimo de impacto.

bot

Uma aplicação de software que executa tarefas automatizadas na internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como crawlers da web que indexam informações na internet. Outros bots, conhecidos como bots maliciosos, têm como objetivo causar disrupção ou danos a indivíduos ou organizações.

botnet

Redes de bots infectadas por malware e sob o controle de uma única parte, conhecidas como bot herder ou operador de bots. Os botnets 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 ramificações (documentação do GitHub).

Acesso de emergência

Em circunstâncias excepcionais e usando um processo aprovado, um meio rápido para um usuário obter acesso a uma Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador Implement break-glass procedures nas orientações do AWS Well-Architected.

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

Veja AWS Cloud Adoption Framework.

implantação canário

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substitui a versão atual por completo.

CCoE

Veja Centro de Excelência da Nuvem.

CDC

Veja captura de dados de alteração.

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 o AWS Fault Injection Service (AWS FIS) para realizar experimentos que estressam suas workloads da AWS e avaliar sua resposta.

CI/CD

Veja integração e 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 feita localmente, antes que o AWS service (Serviço da AWS) de destino os 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 publicações do CCoE no blog Nuvem AWS 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 é normalmente conectada à tecnologia de computação de borda.

modelo operacional em nuvem

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

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam ao migrar para a Nuvem AWS:

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

Essas etapas foram definidas por Stephen Orban na publicação The Journey Toward Cloud-First & the Stages of Adoption no blog Nuvem AWS Enterprise Strategy. Para obter informações sobre como eles se relacionam com a estratégia de migração da AWS, consulte o guia de preparação para migração.

CMDB

Veja 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 o GitHub ou o Bitbucket Cloud. Cada versão do código é chamada de ramificação. Em uma estrutura de microsserviços, cada repositório é dedicado a uma única peça de funcionalidade. Um único pipeline de CI/CD pode usar vários repositórios.

cache frio

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

dados frios

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

visão computacional (CV)

Um campo de IA que usa machine learning para analisar e extrair informações de formatos visuais, como vídeos e imagens digitais. Por exemplo, o Amazon SageMaker AI fornece algoritmos de processamento de imagens para CV.

desvio de configuração

Em uma workload, uma alteração de configuração em relação ao estado esperado. Isso pode fazer com que a workload 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

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

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

desvio de dados

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

dados em trânsito

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

data mesh

Um framework de arquitetura que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

minimização de dados

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

perímetro de dados

Um conjunto de barreiras de proteção preventivas em seu ambiente da AWS que ajudam a garantir que somente suas identidades confiáveis acessem recursos confiáveis das redes esperadas. Para obter mais informações, consulte Building a data perimeter on 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 compatível com business intelligence, como analytics. 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

Veja 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.

defesa completa

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

administrador delegado

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

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

implantação

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

ambiente de desenvolvimento

Veja 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 normalmente são usados para restringir consultas, filtrar e rotular conjuntos de resultados.

desastre

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

Recuperação de desastres (RD)

A estratégia e o processo que você usa para minimizar o tempo de inatividade e a perda de dados causados por um desastre. Para obter mais informações, consulte Recuperação de Workloads em Desastres em AWS: Recuperação na Nuvem na AWS Well-Architected Framework.

DML

Veja 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 recuperação de desastres.

detecção de desvios

Rastreamento de desvios de uma configuração de linha de base. Por exemplo, você pode usar o AWS CloudFormation para detectar desvios nos recursos do sistema ou o AWS Control Tower para detectar alterações em sua zona de pouso que possam afetar a conformidade com os requisitos de governança.

DVSM

Veja mapeamento do fluxo de valor de desenvolvimento.

E

EDA

Veja análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

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

intercâmbio eletrônico de dados (EDI)

A troca automatizada de documentos comerciais entre organizações. Para obter mais informações, consulte O que é EDI (Intercâmbio eletrônico de dados)?.

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja endpoint de serviço.

serviço de endpoint

Um serviço que pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. É possível criar um serviço de endpoint com o AWS PrivateLink e conceder permissões a outras Contas da AWS ou a entidades principais do 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 empresariais (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 envelopada na documentação do AWS Key Management Service (AWS KMS).

ambiente

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

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

epic

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

ERP

Veja planejamento de recursos empresariais.

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. Ela armazena dados quantitativos sobre as operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: as que contêm medidas e as que contêm uma chave externa para uma tabela de dimensões.

antecipar-se à falha

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

delimitação de isolamento contra falhas

Na Nuvem AWS, uma delimitação, como uma zona de disponibilidade, uma Região da AWS, um ambiente de gerenciamento ou um plano de dados, que limita o efeito de uma falha e ajuda a melhorar a resiliência das workloads. Para obter mais informações, consulte AWS Fault Isolation Boundaries.

ramificação de recursos

Veja ramificação.

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 Machine learning model interpretability with 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.

prompts few-shot

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

FGAC

Veja 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 via captura de dados de alteração para migrar os dados no menor tempo possível, em vez de usar uma abordagem em fases. O objetivo é reduzir ao mínimo o tempo de inatividade.

FM

Veja modelo de base.

modelo de base (FM)

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

G

IA generativa

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

bloqueio geográfico

Veja restrições geográficas.

restrições geográficas (bloqueio geográfico)

No Amazon CloudFront, uma opção para impedir que usuários em países específicos acessem distribuições de conteúdo. É possível usar uma lista de permissões ou uma lista de bloqueios para especificar países aprovados e banidos. Para obter mais informações, consulte Como restringir a distribuição geográfica de conteúdo na documentação do CloudFront.

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 trunk-based é a abordagem moderna e preferencial.

golden image

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

estratégia greenfield

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

barreira de proteção

Uma regra de alto nível que ajuda a 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. Elas são implementadas por meio do AWS Config, AWS Security Hub CSPM, Amazon GuardDuty, AWS Trusted Advisor, Amazon Inspector e verificações personalizadas do AWS Lambda.

H

HA

Veja alta disponibilidade.

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

dados de hold-out

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de machine learning. Você pode usar dados de hold-out para avaliar a performance do modelo comparando as predições do modelo com os dados de retenção.

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

eu

IaC

Veja infraestrutura como código.

Política baseada em identidade

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

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 Internet das Coisas Industrial.

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para workloads de produção em vez de atualizar, aplicar patches ou modificar a infraestrutura existente. Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e preditivas do que infraestruturas mutáveis. Para obter mais informações, consulte a prática recomendada Implantar usando infraestrutura imutável no AWS Well-Architected Framework.

VPC de entrada (admissão)

Em uma arquitetura de várias contas da AWS, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de uma aplicação. 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 manufatura por meio de avanços em conectividade, dados em tempo real, automação, analytics 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 várias contas da AWS, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (na mesma ou em diferentes Regiões da AWS), na Internet e em redes on-premises. A Arquitetura de referência de 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 Machine learning model interpretability with AWS.

IoT

Veja 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

Veja biblioteca de informações de TI.

ITSM

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

grande modelo de linguagem (LLM)

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em rótulo.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

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

LLM

Veja grande modelo de linguagem.

ambientes inferiores

Veja 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 ramificação.

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 Troia, spyware e keyloggers.

serviços gerenciados

Serviços da AWS para os quais a 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 abstraídos.

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

Veja Programa de Aceleração da Migração.

mecanismo

Um processo completo em que 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 Building mechanisms no AWS Well-Architected Framework.

conta de membro

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

MES

Veja sistema de execução de manufatura.

Transporte de Telemetria de Enfileiramento de Mensagens (MQTT)

Um protocolo de comunicação leve, máquina a máquina (M2M), baseado no padrão publicar/assinar, 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 Integrar microsserviços usando serviços da AWS sem 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 Implementar microsserviços na AWS.

Programa de Aceleração da Migração (MAP)

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

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

O processo de obter insights sobre o status de preparação de uma organização para a nuvem, identificando pontos fortes e fracos e criar um plano de ação para fechar as lacunas identificadas usando a AWS CAF. 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 workload para a Nuvem AWS. Para obter mais informações, veja a entrada 7 Rs neste glossário e consulte Mobilize your organization to accelerate large-scale migrations.

ML

Veja machine learning.

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 Strategy for modernizing applications in the 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 Evaluating modernization readiness for applications in the Nuvem AWS.

aplicações monolíticas (monólitos)

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

MPA

Veja Avaliação do Portfólio para Migração.

MQTT

Veja 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 workloads de produção. Para melhorar a consistência, confiabilidade e predição, o AWS Well-Architected Framework recomenda o uso de infraestrutura imutável como uma prática recomendada.

U

OAC

Veja controle de acesso de origem.

OAI

Veja identidade de acesso de origem.

OCM

Veja gerenciamento de alterações 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 integração de operações.

OLA

Veja acordo de nível operacional.

migração online

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

OPC-UA

Veja Open Process Communications - Unified Architecture.

Open Process Communications - Unified Architecture (OPC-UA)

Um protocolo de comunicação máquina a máquina (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 práticas recomendadas associadas que ajudam você a entender, avaliar, prevenir ou reduzir o escopo de incidentes e possíveis falhas. Para obter mais informações, consulte Operational Readiness Reviews (ORR) no AWS Well-Architected Framework.

tecnologia operacional (TO)

Sistemas de hardware e software que trabalham com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas de

tecnologia da informação (TI) e tecnologia operacional (TO) é o foco principal das transformações da Indústria 4.0.

integração de operações (OI)

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

trilha organizacional

Uma trilha criada pelo AWS CloudTrail que registra todos os eventos para todas asContas da AWS em uma organização no AWS Organizations. Essa trilha é criada em cada Conta da AWS que faz parte da organização e monitora a atividade em cada conta. Para obter mais informações, consulte Como criar uma trilha para uma organização na documentação do CloudTrail.

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 migração para a AWS, essa estrutura é chamada de aceleração de pessoas devido à velocidade das alterações exigida nos projetos de adoção da nuvem. Para obter mais informações, consulte o guia do OCM.

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

No CloudFront, uma opção para restringir o acesso com o objetivo de proteger seu conteúdo no Amazon S3. Quando você usa o OAI, o CloudFront cria uma entidade principal com a qual o Amazon S3 pode se autenticar. As entidades principais autenticadas podem acessar conteúdo em um bucket do S3 somente por meio de uma distribuição específica do CloudFront. Veja também OAC, que fornece um controle de acesso mais granular e aprimorado.

ORR

Veja análise de prontidão operacional.

OT

Veja tecnologia operacional.

VPC de saída (egresso)

Em uma arquitetura de várias contas da AWS, uma VPC que lida com conexões de rede que são iniciadas de dentro de uma aplicação. 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 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

Veja controlador lógico programável.

PLM

Veja gerenciamento do ciclo de vida do produto.

política

Um objeto que pode definir permissões (veja política baseada em identidade), especificar condições de acesso (veja política baseada em recurso) ou definir as permissões máximas para todas as contas em uma organização no AWS Organizations (veja 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 cláusula `WHERE`.

pushdown de predicados

Uma técnica de otimização de consultas 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 a performance 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.

entidade principal

Entidade na AWS que pode executar ações e acessar recursos. Essa entidade geralmente é um usuário raiz de uma Conta da AWS, um perfil do IAM ou um usuário. Para obter mais

informações, consulte Entidade principal em Termos e conceitos de perfis na documentação do IAM.

privacidade desde a concepção

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

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 desenvolvido para evitar a implantação de recursos não conformes. Esses controles verificam 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 documentação do AWS Control Tower e Proactive controls em Implementing security controls on 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 a concepção, o desenvolvimento e o lançamento, passando pelo crescimento e maturidade, até o declínio e a remoção.

ambiente de produção

Veja ambiente.

controlador lógico programável (PLC)

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

encadeamento de prompts

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

pseudonimização

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

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 em que outros microsserviços possam assinar. 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, aprovador, consultado, informado (RACI).

RAG

Veja geração aumentada via recuperação.

ransomware

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

Matriz RASCI

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

RCAC

Veja controle de acesso por linha e coluna.

réplica de leitura

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

reestruturar a arquitetura

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

região

Uma coleção de recursos da AWS em uma área geográfica. Cada Região da AWS é isolada e independente das demais para fornecer tolerância a falhas, estabilidade e resiliência. Para obter informações, consulte Specify which Regiões da AWS your account can use.

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 uma aplicação de resistir ou se recuperar de interrupções. Alta disponibilidade e recuperação de desastres são considerações comuns ao planejar a resiliência na Nuvem AWS. Para obter mais informações, consulte Nuvem AWS Resilience.

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.

retirar

Veja 7 Rs.

Geração Aumentada de Recuperação (RAG)

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

alternância

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

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 objetivo de ponto de recuperação.

RTO

Veja objetivo de 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 usado por muitos provedores de identidade (IdPs). Esse recurso permite a autenticação única (SSO) federada para que os usuários possam fazer login no Console de

gerenciamento da AWS ou chamar as operações de API da AWS 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 política de controle de serviço.

secret

No AWS Secrets Manager, informações sensíveis ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. 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 What's in a Secrets Manager secret? na documentação do Secrets Manager.

segurança desde a concepção

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

controle de segurança

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

hardening 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 práticas recomendadas de segurança da AWS. Exemplos de ações de resposta automatizada incluem a modificação de um grupo de segurança da VPC, a aplicação de patches em uma instância do Amazon EC2 ou a alternância de credenciais.

Criptografia do lado do servidor

A criptografia dos dados no destino pelo AWS service (Serviço da AWS) que 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 serviços na documentação do AWS Organizations.

service endpoint (endpoint de serviço)

O URL do ponto de entrada de 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 avaliação de um aspecto de performance de um serviço, como taxa de erro, disponibilidade ou throughput.

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

Um modelo que descreve a responsabilidade que você compartilha com a AWS em questões de segurança e conformidade na nuvem. A 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 sistema de gerenciamento de eventos e informações de segurança.

ponto único de falha (SPOF)

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

SLA

Veja acordo de serviço.

SLI

Veja indicador de nível de serviço.

SLO

Veja objetivo de nível de serviço.

modelo dividir e semear

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 Phased approach to modernizing applications in the Nuvem AWS.

SPOF

Veja ponto único de falha.

esquema em estrela

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 ser usada em um data warehouse ou para fins de inteligência comercial.

padrão strangler fig

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

sub-rede

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

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

prompt do sistema

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja 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 documentação do AWS Transit Gateway.

fluxo de trabalho baseado em troncos

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

Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização no AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas

de gerenciamento para você. Para obter mais informações, consulte Como usar o AWS Organizations com outros serviços da AWS na documentação do AWS Organizations.

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja 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 backend.

workstreams

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

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

WORM

Veja gravação única e várias leituras.

WQF

Veja AWS Workload Qualification Framework.

gravação única e várias leituras (WORM)

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

Z

exploração de dia zero

Um ataque, normalmente malware, que tira proveito de uma vulnerabilidade zero-day.

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.

prompts zero-shot

Fornecer a um LLM instruções para realizar uma tarefa, mas sem exemplos (shots) que possam ajudar a orientá-lo. O LLM deve usar seu conhecimento pré-treinado para lidar com a tarefa. A eficácia dos prompts zero-shot depende da complexidade da tarefa e da qualidade do prompt. Veja também prompts few-shot.

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.