Projetando e implementando o registro e o monitoramento com a Amazon CloudWatch

AWS Orientação prescritiva

AWS Orientação prescritiva: Projetando e implementando o registro e o monitoramento com a Amazon CloudWatch

Table of Contents

Projetando e implementando registros e monitoramento com a Amazon CloudWatch

Khurram Nizami, Amazon Web Services (AWS)

Abril de 2023 (histórico do documento)

Este guia ajuda você a projetar e implementar registros e monitoramento com a Amazon CloudWatch e os serviços relacionados de gerenciamento e governança da Amazon Web Services (AWS) para cargas de trabalho que usam instâncias do Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) e servidores locais. AWS Lambda O guia é destinado a equipes de operações, DevOps engenheiros e engenheiros de aplicativos que gerenciam cargas de trabalho naAWS nuvem.

Sua abordagem de registro e monitoramento deve ser baseada nos seis pilares doAWS Well-Architected Framework. Esses pilares são excelência operacional, segurança, confiabilidade, eficiência de desempenho e otimização de custos. Uma solução de monitoramento e alarme bem arquitetada melhora a confiabilidade e o desempenho, ajudando você a analisar e ajustar proativamente sua infraestrutura.

Este guia não discute extensivamente o registro e o monitoramento para segurança ou otimização de custos, pois esses são tópicos que exigem uma avaliação aprofundada. Existem muitosAWS serviços que oferecem suporte ao registro e monitoramento de segurança AWS CloudTrailAWS Config, incluindo Amazon Inspector, Amazon Detective, Amazon Macie GuardDuty AWS Security Hub, Amazon e. Você também pode usar AWS Cost ExplorerAWSorçamentos e métricas deCloudWatch faturamento para otimização de custos.

A tabela a seguir descreve as seis áreas que sua solução de registro e monitoramento deve abordar.

Capturando e ingerindo arquivos de log e métricas	Identifique, configure e envie registros e métricas do sistema e do aplicativo paraAWS serviços de diferentes fontes.
Pesquisando e analisando registros	Pesquise e analise registros para gerenciam ento de operações, identificação de problemas, solução de problemas e análise de aplicativos.

Métricas de monitoramento e alarmes	Identifique e atue de acordo com as observaçõ es e tendências em suas cargas de trabalho.
Monitorando a disponibilidade de aplicativos e serviços	Reduza o tempo de inatividade e melhore sua capacidade de atingir as metas de nível de serviço monitorando continuamente a disponibi lidade do serviço.
Aplicativos de rastreamento	Rastreie solicitações de aplicativos em sistemas e dependências externas para ajustar o desempenho, realizar análises de causas básicas e solucionar problemas.
Criação de painéis e visualizações	Crie painéis que se concentrem em métricas e observações relevantes para seus sistemas e cargas de trabalho, o que ajuda na melhoria contínua e na descoberta proativa de problemas.

CloudWatch pode atender à maioria dos requisitos de registro e monitoramento e fornece uma solução confiável, escalável e flexível. MuitosAWS serviços fornecem CloudWatch métricas automaticamente, além da integração de CloudWatch registros para monitoramento e análise. CloudWatch também fornece agentes e drivers de registro para dar suporte a uma variedade de opções de computação, como servidores (na nuvem e no local), contêineres e computação sem servidor. Este guia também aborda os seguintesAWS serviços usados com registro e monitoramento:

- AWS Systems ManagerDistribuidor, Systems Manager, gerente de estado e Systems Manager: automação para automatizar, configurar e atualizar o CloudWatch agente para suas instâncias do EC2 e servidores locais
- Amazon OpenSearch Service para agregação, pesquisa e análise avançadas de registros
- Verificações de saúde e CloudWatchSynthetics Amazon Route 53 para monitorar a disponibilidade de aplicativos e serviços
- Amazon Managed Service for Prometheus para monitorar aplicativos em contêineres em grande escala
- AWS X-Raypara rastreamento de aplicativos e análise de tempo de execução

- Amazon Managed Grafana para visualizar e analisar dados de várias fontes (por exemplo CloudWatch, Amazon OpenSearch Service e Amazon Timestream)

Os serviços deAWS computação que você escolhe também afetam a implementação e a configuração da sua solução de registro e monitoramento. Por exemplo, CloudWatch a implementação e a configuração do Amazon EC2, Amazon ECS, Amazon EKS e Lambda são diferentes.

Os proprietários de aplicativos e cargas de trabalho geralmente podem esquecer o registro e o monitoramento ou configurá-los e implementá-los de forma inconsistente. Isso significa que as cargas de trabalho entram em produção com observabilidade limitada, o que causa atrasos na identificação de problemas e aumenta o tempo necessário para solucioná-los e resolvê-los. No mínimo, sua solução de registro e monitoramento deve abordar a camada de sistemas para os registros e métricas no nível do sistema operacional (OS), além da camada de aplicativo para registros e métricas do aplicativo. O guia fornece uma abordagem recomendada para abordar essas duas camadas em diferentes tipos de computação, incluindo os três tipos de computação descritos na tabela a seguir.

Instâncias EC2 imutáveis e de longa duração	Registros e métricas de sistemas e aplicativos em vários sistemas operacionais (OSs) em váriasAWS regiões ou contas.
Contêineres	Registros e métricas do sistema e do aplicativo para seus clusters do Amazon ECS e do Amazon EKS, incluindo exemplos para diferentes configurações.
Sem servidor	Registros e métricas do sistema e do aplicativo para suas funções do Lambda e considerações para personalização.

Este guia fornece uma solução de registro e monitoramento que CloudWatch abordaAWS serviços relacionados nas seguintes áreas:

- Planejando sua CloudWatch implantação— Considerações para planejar sua CloudWatch implantação e orientação sobre como centralizar sua CloudWatch configuração.

- Configurar a CloudWatch Agente para instâncias do EC2 e servidores on-premises— detalhes de CloudWatch configuração para registros e métricas em nível de sistema e aplicativo.
- Abordagens de instalação do agente CloudWatch para servidores Amazon EC2 e locais— Abordagens para instalar o CloudWatch agente, incluindo implantação automatizada usando o Systems Manager em várias regiões e contas.
- Registro e monitoramento no Amazon ECS — Orientação CloudWatch para configuração de registros e métricas em nível de cluster e de aplicativo no Amazon ECS.
- Registro em log e monitoramento no Amazon EKS — Orientação para configuração CloudWatch de registros e métricas em nível de cluster e de aplicativo no Amazon EKS.
- Monitoramento do Prometheus no Amazon EKS— Apresenta e compara o Amazon Managed Service for Prometheus com o monitoramento do CloudWatch Container Insights para o Prometheus.
- Registro e métricas paraAWS Lambda— Orientação CloudWatch para configurar suas funções do Lambda.
- Pesquisando e analisando registros CloudWatch— Métodos para analisar seus registros usando Amazon CloudWatch Application Insights, CloudWatch Logs Insights e estender a análise de registros para o Amazon OpenSearch Service.
- Opções alarmantes com o CloudWatch— Apresenta CloudWatch alarmes e detecção de CloudWatch anomalias e fornece orientação sobre a criação e configuração de alarmes.
- Monitoramento da disponibilidade de aplicativos e serviços— Apresenta e compara as verificações de integridade CloudWatch do Synthetics e do Route 53 para monitoramento automatizado da disponibilidade.
- Aplicações de rastreamento comAWS X-Ray— Introdução e configuração do rastreamento de aplicativos usando o X-Ray para Amazon EC2, Amazon ECS, Amazon EKS e Lambda
- Painéis e visualizações com o CloudWatch— Introdução aos CloudWatch painéis para melhorar a observabilidade em todas asAWS cargas de trabalho.
- Integração do CloudWatch com oAWSserviços— Explica como CloudWatch se integra a váriosAWS serviços.
- Amazon Managed Grafana para painéis e visualização— Apresenta e compara o Amazon Managed Grafana com o Amazon CloudWatch para painéis e visualização.

Exemplos de implementação são usados em todo este guia nessas áreas e também estão disponíveis no GitHub repositórioAWS Samples.

Resultados de negócios direcionados

Criando uma solução de registro e monitoramento projetada para oAWSA nuvem é essencial para alcançar oseis vantagens da computação em nuvem. Sua solução de registro e monitoramento deve ajudar sua organização de TI a alcançar resultados de negócios que beneficiem seus processos de negócios, parceiros de negócios, funcionários e clientes. Você pode esperar os quatro resultados a seguir após a implementação de uma solução de registro e monitoramento alinhada com oAWSEstrutura Well-Architected:

Acelere a disponibilidade operacional

Habilitar uma solução de registro e monitoramento é um componente importante da preparação de uma carga de trabalho para suporte e uso de produção. A prontidão operacional pode rapidamente se tornar um gargalo se você confiar muito em processos manuais e também reduzir o tempo de retorno (TTV) para seus investimentos em TI. Uma abordagem ineficaz também resulta em observabilidade limitada de suas cargas de trabalho. Isso pode aumentar o risco de interrupções prolongadas, insatisfação do cliente e processos de negócios falhados.

Você pode usar as abordagens deste guia para padronizar e automatizar seu registro e monitoramento noAWSNuvem. Novas cargas de trabalho requerem preparação e intervenção manuais mínimas para registro e monitoramento de produção. Isso também ajuda a reduzir o tempo e as etapas necessárias para criar padrões de registro e monitoramento em escala para diferentes cargas de trabalho em várias contas e regiões.

Melhore a Excelência operacional

Este guia fornece várias práticas recomendadas para registro e monitoramento que ajudam diversas cargas de trabalho a atingir os objetivos de negócios eExcelência operacional. Este guia também forneceexemplos detalhados e modelos reutilizáveis de código abertoque você pode usar com uma abordagem de infraestrutura como código (IaC) para implementar uma solução de monitoramento e registro bem arquitetada usandoAWSServiços da . Melhorar a excelência operacional é iterativo e requer melhoria contínua. O guia fornece sugestões sobre como melhorar continuamente as práticas de registro e monitoramento.

Melhore a visibilidade operacional

Seus processos e aplicativos de negócios podem ser suportados por diferentes recursos de TI e hospedados em diferentes tipos de computação, no local ou noAWSNuvem. Sua visibilidade operacional pode ser limitada por implementações inconsistentes e incompletas de sua estratégia de registro e monitoramento. A adoção de uma abordagem abrangente de registro e monitoramento ajuda a identificar, diagnosticar e responder rapidamente a problemas em suas cargas de trabalho. Este guia ajuda você a projetar e implementar abordagens para melhorar sua visibilidade operacional completa e reduzir o tempo médio para resolver falhas (MTTR). Uma abordagem abrangente de registro e monitoramento também ajuda sua organização a melhorar a qualidade do serviço, aprimorar a experiência do usuário final e cumprir contratos de nível de serviço (SLAs).

Dimensione as operações e reduza custos indiretos

Você pode dimensionar as práticas de registro e monitoramento a partir deste guia para oferecer suporte a várias regiões e contas, recursos de curta duração e vários ambientes. O guia fornece abordagens e exemplos para automatizar etapas manuais (por exemplo, instalar e configurar agentes, monitorar métricas e notificar ou agir quando ocorrem problemas). Essas abordagens são úteis quando a adoção da nuvem amadurece e cresce e você precisa dimensionar a capacidade operacional sem aumentar as atividades ou recursos de gerenciamento de nuvem.

Planejando sua CloudWatch implantação

A complexidade e o escopo de uma solução de registro e monitoramento dependem de vários fatores, incluindo:

- Quantos ambientes, regiões e contas são usados e como esse número pode aumentar.
- A variedade e os tipos de suas cargas de trabalho e arquiteturas existentes.
- Os tipos de computação e sistemas operacionais que devem ser registrados e monitorados.
- Se há locais e AWS infraestrutura locais.
- Os requisitos analíticos e de agregação de vários sistemas e aplicativos.
- Requisitos de segurança que evitam a exposição não autorizada de registros e métricas.
- Produtos e soluções que devem ser integrados à sua solução de registro e monitoramento para dar suporte aos processos operacionais.

Você deve revisar e atualizar regularmente sua solução de registro e monitoramento com implantações de carga de trabalho novas ou atualizadas. As atualizações em seu registro, monitoramento e alarme devem ser identificadas e aplicadas quando problemas são observados. Esses problemas podem então ser identificados e evitados de forma proativa no futuro.

Você deve se certificar de instalar e configurar consistentemente software e serviços para capturar e ingerir registros e métricas. Uma abordagem estabelecida de registro e monitoramento usa serviços e soluções de fornecedores de software (ISV) múltiplos AWS ou independentes para diferentes domínios (por exemplo, segurança, desempenho, rede ou análise). Cada domínio tem seus próprios requisitos de implantação e configuração.

Recomendamos usar CloudWatch para capturar e ingerir registros e métricas de vários sistemas operacionais e tipos de computação. Muitos AWS serviços são usados CloudWatch para registrar, monitorar e publicar registros e métricas, sem a necessidade de configuração adicional. CloudWatch fornece um agente de software que pode ser instalado e configurado para diferentes sistemas operacionais e ambientes. As seções a seguir descrevem como implantar, instalar e configurar o CloudWatch agente para várias contas, regiões e configurações:

Tópicos

Uso CloudWatch em contas centralizadas ou distribuídas

Embora tenha sido CloudWatch projetado para monitorar AWS serviços ou recursos em uma conta e região, você pode usar uma conta central para capturar registros e métricas de várias contas e regiões. Se você usa mais de uma conta ou região, deve avaliar se deve usar a abordagem de conta centralizada ou uma conta individual para capturar registros e métricas. Normalmente, uma abordagem híbrida é necessária para implantações em várias contas e em várias regiões para atender aos requisitos de segurança, análise, operações e proprietários de cargas de trabalho.

A tabela a seguir fornece áreas a serem consideradas ao escolher usar uma abordagem centralizada, distribuída ou híbrida.

Estruturas de contas	Sua organização pode ter várias contas separadas (por exemplo, contas para cargas de trabalho não produtivas e de produção) ou milhares de contas para aplicativos únicos em ambientes específicos. Recomendamos que você mantenha registros e métricas do aplicativo na conta em que a carga de trabalho é executada, o que dá aos proprietários da carga de trabalho acesso aos registros e métricas. Isso permite que eles tenham um papel ativo no registro e no monitoramento. Também recomendamos que você use uma conta de registro separada para agregar todos os registros de carga de trabalho para análise, agregação, tendências e operações centralizadas. Contas de registro separadas também podem ser usadas para segurança, arquivamento, monitoramento e análise.
Requisitos de acesso	Os membros da equipe (por exemplo, proprietários de cargas de trabalho ou desenvolvedores) precisam de acesso a registros e métricas para solucionar problemas e fazer melhorias. Os registros devem ser mantidos na conta da carga de trabalho para facilitar o acesso e a solução de problemas. Se os registros e as métricas forem mantidos em uma conta separada da carga de trabalho, talvez os usuários precisem alternar regularmente entre contas. O uso de uma conta centralizada fornece informações de registro para usuários autorizados sem conceder acesso à conta de carga de trabalho. Isso pode simplificar os requisitos de acesso para

	cargas de trabalho analíticas em que a agregação é necessári a de cargas de trabalho executadas em várias contas. A conta de registro centralizada também pode ter opções alternativas de busca e agregação, como um cluster do Amazon OpenSearch Service. O Amazon OpenSearch Service fornece controle de acesso refinado até o nível do campo para seus registros. O controle de acesso refinado é importante quando você tem dados sensíveis ou confidenciais que exigem acesso e permissões especializados.
Operações	Muitas organizações têm uma equipe centralizada de operações e segurança ou uma organização externa para suporte operacion al que requer acesso aos registros para monitoramento. O registro e o monitoramento centralizados podem facilitar a identificação de tendências, a pesquisa, a agregação e a realização de análises em todas as contas e cargas de trabalho. Se sua organização usa a abordagem "você cria, você executa" DevOps, os proprietários da carga de trabalho precisam registrar e monitorar as informações em suas contas. Pode ser necessária uma abordagem híbrida para satisfazer as operações e análises centrais, além da propriedade distribuída da carga de trabalho.
Ambiente	Você pode escolher hospedar registros e métricas em um local central para contas de produção e manter registros e métricas para outros ambientes (por exemplo, desenvolvimento ou teste) na mesma conta ou em contas separadas, dependendo dos requisito s de segurança e da arquitetura da conta. Isso ajuda a evitar que dados confidenciais criados durante a produção sejam acessados por um público mais amplo.

CloudWatch fornece várias opções para processar registros em tempo real com filtros de CloudWatch assinatura. Você pode usar filtros de assinatura para transmitir registros em tempo real para AWS serviços de processamento, análise e carregamento personalizados em outros sistemas. Isso pode ser particularmente útil se você adotar uma abordagem híbrida em que seus

registros e métricas estejam disponíveis em contas e regiões individuais, além de uma conta e região centralizadas. A lista a seguir fornece exemplos de AWS serviços que podem ser usados para isso:

- Amazon Data Firehose — O Firehose fornece uma solução de streaming que escala e redimensiona automaticamente com base no volume de dados que está sendo produzido. Você não precisa gerenciar o número de fragmentos em um stream de dados do Amazon Kinesis e pode se conectar diretamente ao Amazon Simple Storage Service (Amazon S3) OpenSearch , Amazon Service ou Amazon Redshift sem codificação adicional. O Firehose é uma solução eficaz se você quiser centralizar seus registros nesses serviços. AWS
- Amazon Kinesis Data Streams — O Kinesis Data Streams é uma solução adequada se você precisar se integrar a um serviço ao qual o Firehose não oferece suporte e implementar lógica de processamento adicional. Você pode criar um destino do Amazon CloudWatch Logs em suas contas e regiões que especifica um stream de dados do Kinesis em uma conta central e AWS Identity and Access Management uma função (IAM) que concede permissão para colocar registros no stream. O Kinesis Data Streams fornece uma landing zone flexível e aberta para seus dados de log, que pode então ser consumida por diferentes opções. Você pode ler os dados de log do Kinesis Data Streams em sua conta, realizar o pré-processamento e enviar os dados para o destino escolhido.

  No entanto, você deve configurar os fragmentos do stream para que ele seja dimensionado adequadamente para os dados de log produzidos. O Kinesis Data Streams atua como intermediário temporário ou fila para seus dados de log, e você pode armazenar os dados no stream do Kinesis por entre um e 365 dias. O Kinesis Data Streams também oferece suporte ao recurso de repetição, o que significa que você pode reproduzir dados que não foram consumidos.
- Amazon OpenSearch Service — CloudWatch Os registros podem transmitir registros em um grupo de registros para um OpenSearch cluster em uma conta individual ou centralizada. Quando você configura um grupo de registros para transmitir dados para um OpenSearch cluster, uma função Lambda é criada na mesma conta e região do seu grupo de registros. A função Lambda deve ter uma conexão de rede com o OpenSearch cluster. Você pode personalizar a função Lambda para realizar um pré-processamento adicional, além de personalizar a ingestão no Amazon Service. OpenSearch O registro centralizado com o Amazon OpenSearch Service facilita a análise, a pesquisa e a solução de problemas em vários componentes em sua arquitetura de nuvem.
- Lambda — Se você usa o Kinesis Data Streams, precisa provisionar e gerenciar recursos computacionais que consomem dados do seu stream. Para evitar isso, você pode transmitir dados de log diretamente para o Lambda para processamento e enviá-los para um destino com base na sua lógica. Isso significa que você não precisa provisionar e gerenciar recursos computacionais

para processar os dados recebidos. Se você optar por usar o Lambda, certifique-se de que sua solução seja compatível com as cotas do Lambda.

Talvez seja necessário processar ou compartilhar dados de registro armazenados em CloudWatch Registros em formato de arquivo. Você pode criar uma tarefa de exportação para exportar um grupo de logs para o Amazon S3 em uma data ou intervalo de tempo específico. Por exemplo, você pode optar por exportar registros diariamente para o Amazon S3 para análise e auditoria. O Lambda pode ser usado para automatizar essa solução. Você também pode combinar essa solução com a replicação do Amazon S3 para enviar e centralizar seus registros de várias contas e regiões para uma conta e região centralizadas.

A configuração do CloudWatch agente também pode especificar um `credentials` campo na `agent`seção. Isso especifica uma função do IAM a ser usada ao enviar métricas e registros para uma conta diferente. Se especificado, esse campo contém o `role_arn` parâmetro. Esse campo pode ser usado quando você só precisa de registro e monitoramento centralizados em uma conta e região centralizadas específicas.

Você também pode usar o AWS SDK para escrever seu próprio aplicativo de processamento personalizado em um idioma de sua escolha, ler registros e métricas de suas contas e enviar dados para uma conta centralizada ou outro destino para processamento e monitoramento adicionais.

Gerenciando arquivos de configuração do CloudWatch agente

Recomendamos que você crie uma configuração padrão de CloudWatch agente da Amazon que inclua os registros e métricas do sistema que você deseja capturar em todas as suas instâncias e servidores locais do Amazon Elastic Compute Cloud (Amazon EC2). Você pode usar o assistente do arquivo de configuração do CloudWatch agente para ajudá-lo a criar o arquivo de configuração. Você pode executar o assistente de configuração várias vezes para gerar configurações exclusivas para diferentes sistemas e ambientes. Você também pode modificar o arquivo de configuração ou criar variações usando o esquema do arquivo de configuração. O arquivo de configuração do CloudWatch agente pode ser armazenado nos parâmetros do AWS Systems Manager Parameter Store. Você pode criar parâmetros separados do Parameter Store se tiver vários arquivos de configuração do CloudWatch agente. Se você estiver usando várias contas da AWS ou regiões da AWS, deverá gerenciar e atualizar os parâmetros do Parameter Store em cada conta e região. Como alternativa, você pode gerenciar centralmente suas CloudWatch configurações como arquivos no Amazon S3 ou em uma ferramenta de controle de versão de sua escolha.

O `amazon-cloudwatch-agent-ctl` script incluído no CloudWatch agente permite que você especifique um arquivo de configuração, um parâmetro do Parameter Store ou a configuração padrão do agente. A configuração padrão se alinha ao conjunto de métricas básico e predefinido e configura o agente para o qual reportar métricas de memória e espaço em disco. CloudWatch No entanto, ele não inclui nenhuma configuração de arquivo de log. A configuração padrão também será aplicada se você usar o Systems Manager Quick Setup para o CloudWatch agente.

Como a configuração padrão não inclui registro e não é personalizada para seus requisitos, recomendamos que você crie e aplique suas próprias CloudWatch configurações, personalizadas de acordo com seus requisitos.

Gerenciando CloudWatch configurações

Por padrão, CloudWatch as configurações podem ser armazenadas e aplicadas como parâmetros do Parameter Store ou como arquivos CloudWatch de configuração. A melhor escolha dependerá de suas necessidades. Nesta seção, discutiremos os prós e os contras dessas duas opções. Uma solução representativa também é detalhada para gerenciar arquivos de CloudWatch configuração para várias contas e regiões da AWS.

Parâmetros do Systems Manager Parameter Store

Usar os parâmetros do Parameter Store para gerenciar CloudWatch configurações funciona bem se você tiver um único arquivo de configuração de CloudWatch agente padrão que deseja aplicar e gerenciar em um pequeno conjunto de contas e regiões da AWS. Ao armazenar suas CloudWatch configurações como parâmetros do Parameter Store, você pode usar a ferramenta de configuração do CloudWatch agente (`amazon-cloudwatch-agent-ctl`no Linux) para ler e aplicar a configuração do Parameter Store sem precisar copiar o arquivo de configuração para sua instância. Você pode usar o documento AmazonCloudWatch- ManageAgent Systems Manager Command para atualizar a CloudWatch configuração em várias instâncias do EC2 em uma única execução. Como os parâmetros do Parameter Store são regionais, você deve atualizar e manter os parâmetros do CloudWatch Parameter Store em cada região da AWS e conta da AWS. Se você tiver várias CloudWatch configurações que deseja aplicar a cada instância, deverá personalizar o documento AmazonCloudWatch- ManageAgent Command para incluir esses parâmetros.

CloudWatch arquivos de configuração

Gerenciar suas CloudWatch configurações como arquivos pode funcionar bem se você tiver muitas contas e regiões da AWS e estiver gerenciando vários arquivos de CloudWatch configuração. Usando essa abordagem, você pode navegar, organizar e gerenciá-los em uma estrutura de pastas.

Você pode aplicar regras de segurança a pastas ou arquivos individuais para limitar e conceder acesso, como permissões de atualização e leitura. Você pode compartilhá-los e transferi-los para fora da AWS para colaboração. Você pode controlar a versão dos arquivos para rastrear e gerenciar as alterações. Você pode aplicar CloudWatch configurações coletivamente copiando os arquivos de configuração para o diretório de configuração do CloudWatch agente sem aplicar cada arquivo de configuração individualmente. Para Linux, o diretório CloudWatch de configuração é encontrado em`/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d`. Para Windows, o diretório de configuração é encontrado em`C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs`.

Quando você inicia o CloudWatch agente, o agente anexa automaticamente cada arquivo encontrado nesses diretórios para criar um arquivo de configuração CloudWatch composto. Os arquivos de configuração devem ser armazenados em um local central (por exemplo, um bucket S3) que possa ser acessado pelas contas e regiões necessárias. Um exemplo de solução usando essa abordagem é fornecido.

Organizando CloudWatch configurações

Independentemente da abordagem usada para gerenciar suas CloudWatch configurações, organize suas CloudWatch configurações. Você pode organizar suas configurações em caminhos de arquivo ou de armazenamento de parâmetros usando uma abordagem como a seguinte.

/config/standard/windows/ec2	Armazene arquivos de CloudWatch configuração padrão específicos do Windows para o Amazon EC2. Você pode categorizar ainda mais suas configurações padrão de sistema operacional (SO) para diferentes versões do Windows, tipos de instância EC2 e ambientes nesta pasta.
/config/standard/windows/no local	Armazene arquivos de CloudWatch configuração padrão específicos do Windows para servidores locais. Você também categoriza ainda mais suas configurações de sistema operacional padrão para diferentes versões, tipos de servidores e ambientes do Windows nessa pasta.

/config/standard/linux/ec2	Armazene seus arquivos de CloudWatch configuração padrão específicos do Linux para o Amazon EC2. Você pode categorizar ainda mais sua configuração de sistema operacional padrão para diferentes distribuições Linux, tipos de instância EC2 e ambientes nesta pasta.
/config/standard/linux/no local	Armazene seus arquivos de CloudWatch configuração padrão específicos do Linux para servidores locais. Você pode categorizar ainda mais a configuração padrão do sistema operacional para diferentes distribuições, tipos de servidores e ambientes Linux nesta pasta.
/config/ecs	Armazene arquivos de CloudWatch configura ção específicos do Amazon Elastic Container Service (Amazon ECS) se você usar instâncias de contêiner do Amazon ECS. Essas configura ções podem ser anexadas às configura ções padrão do Amazon EC2 para registro e monitoramento específicos em nível de sistema do Amazon ECS.
/config/ <application_name>	Armazene seus arquivos de configuração específicos do aplicativo CloudWatch . Você pode categorizar ainda mais seus aplicativ os com pastas e prefixos adicionais para ambientes e versões.

Exemplo: armazenamento de arquivos CloudWatch de configuração em um bucket do S3

Esta seção fornece um exemplo do uso do Amazon S3 para armazenar arquivos de CloudWatch configuração e um runbook personalizado do Systems Manager para recuperar e aplicar os arquivos de configuração. CloudWatch Essa abordagem pode resolver alguns dos desafios de usar os parâmetros do Systems Manager Parameter Store para CloudWatch configuração em grande escala:

- Se você usar várias regiões, deverá sincronizar as atualizações de CloudWatch configuração no repositório de parâmetros de cada região. O Parameter Store é um serviço regional e o mesmo parâmetro deve ser atualizado em cada região que usa o CloudWatch agente.
- Se você tiver várias CloudWatch configurações, deverá iniciar a recuperação e a aplicação de cada configuração do Parameter Store. Você deve recuperar individualmente cada CloudWatch configuração do Parameter Store e também atualizar o método de recuperação sempre que adicionar uma nova configuração. Por outro lado, CloudWatch fornece um diretório de configuração para armazenar arquivos de configuração e aplica cada configuração no diretório, sem exigir que sejam especificados individualmente.
- Se você usa várias contas, deve garantir que cada nova conta tenha as CloudWatch configurações necessárias em seu Parameter Store. Você também precisa se certificar de que todas as alterações de configuração sejam aplicadas a essas contas e suas regiões no futuro.

Você pode armazenar CloudWatch configurações em um bucket do S3 que pode ser acessado de todas as suas contas e regiões. Em seguida, você pode copiar essas configurações do bucket do S3 para o diretório de CloudWatch configuração usando os runbooks do Systems Manager Automation e o Systems Manager State Manager. Você pode usar o modelo cloudwatch-config-s3-bucket.yaml da CloudFormation AWS para criar um bucket do S3 que pode ser acessado por várias contas dentro de uma organização no AWS Organizations. O modelo inclui um `OrganizationID` parâmetro que concede acesso de leitura a todas as contas da sua organização.

A amostra aumentada do runbook do Systems Manager, fornecida na seção Configurar o Gerenciador Estadual e Distribuidor para implantação e configuração de CloudWatch agentes deste guia, está configurada para recuperar arquivos usando o bucket S3 criado pelo modelo AWS 3-bucket.yaml. cloudwatch-config-s CloudFormation

Como alternativa, você pode usar um sistema de controle de versão (por exemplo, GitHub ou AWS CodeCommit) para armazenar seus arquivos de configuração. Se você quiser recuperar automaticamente os arquivos de configuração armazenados em um sistema de controle de versão, precisará gerenciar ou centralizar o armazenamento de credenciais e atualizar o runbook do Systems Manager Automation usado para recuperar as credenciais em suas contas e regiões.

Configurar a CloudWatch Agente para instâncias do EC2 e servidores on-premises

Muitas organizações executam cargas de trabalho em servidores físicos e máquinas virtuais (VMs). Essas cargas de trabalho normalmente são executadas em sistemas operacionais diferentes, cada um com requisitos exclusivos de instalação e configuração para capturar e ingerir métricas.

Se você optar por usar instâncias do EC2, poderá ter um alto nível de controle sobre sua instância e a configuração do sistema operacional. No entanto, esse nível mais alto de controle e responsabilidade exige que você monitore e ajuste as configurações para obter um uso mais eficiente. Você pode melhorar sua eficácia operacional estabelecendo padrões para registro e monitoramento e aplicando uma abordagem padrão de instalação e configuração para capturar e ingerir registros e métricas.

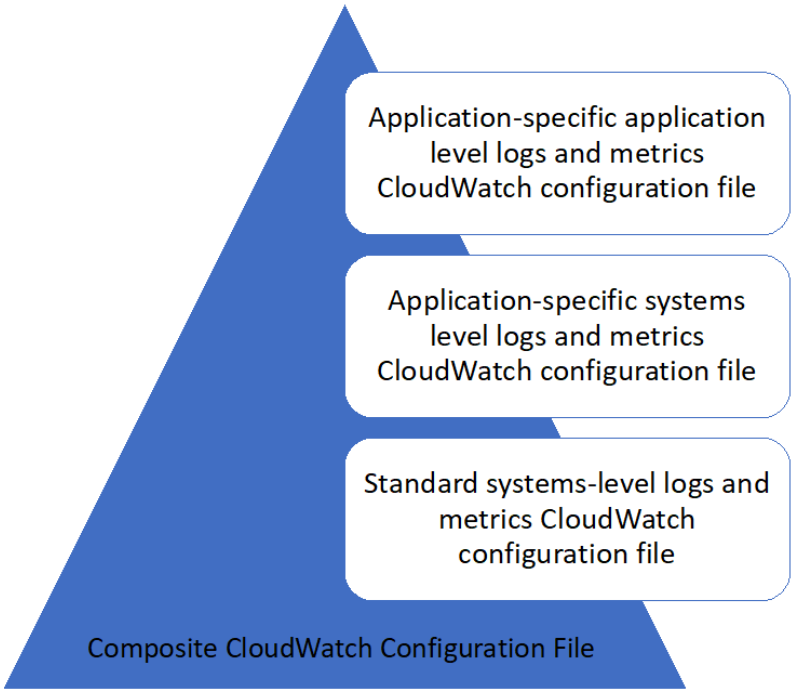
Organizations que migram ou estendem seus investimentos em TI para oAWSA nuvem pode aproveitar CloudWatch para obter uma solução unificada de registro e monitoramento. CloudWatch preços significa que você paga incrementalmente pelas métricas e registros que deseja capturar. Você também pode capturar registros e métricas para servidores locais usando um similar CloudWatch processo de instalação do agente como aquele para o Amazon EC2.

Antes de começar a instalar e implantar o CloudWatch, verifique se você avaliou as configurações de registro e métricas para seus sistemas e aplicativos. Certifique-se de definir os logs e as métricas padrão que você precisa capturar para os sistemas operacionais que deseja usar. Os logs e as métricas do sistema são a base e o padrão para uma solução de registro e monitoramento porque são gerados pelo sistema operacional e são diferentes para Linux e Windows. Existem métricas importantes e arquivos de log disponíveis nas distribuições Linux, além daqueles que são específicos para uma versão ou distribuição do Linux. Essa variação também ocorre entre diferentes versões do Windows.

Configurar a CloudWatch agente

O CloudWatch captura métricas e logs do Amazon EC2 e servidores on-premises usandoAgentes do CloudWatch e arquivos de configuração do agenteSão específicos de cada sistema operacional. Recomendamos que você defina a métrica padrão e a configuração de captura de log da sua organização antes de começar a instalar o CloudWatch agente em escala em suas contas.

Você pode combinar vários CloudWatch configurações de agente para formar um composto CloudWatch Configuração do agente. Uma abordagem recomendada é definir e dividir configurações para seus registros e métricas no nível do sistema e do aplicativo. O diagrama a seguir ilustra como vários tipos de arquivos de configuração do CloudWatch para diferentes requisitos podem ser combinados para formar uma configuração composta do CloudWatch:



Esses registros e métricas também podem ser classificados e configurados para ambientes ou requisitos específicos. Por exemplo, você pode definir um subconjunto menor de registros e métricas com menor precisão para ambientes de desenvolvimento não regulamentados e um conjunto maior e mais completo com maior precisão para ambientes de produção regulamentados.

Configurando a captura de log para instâncias do EC2

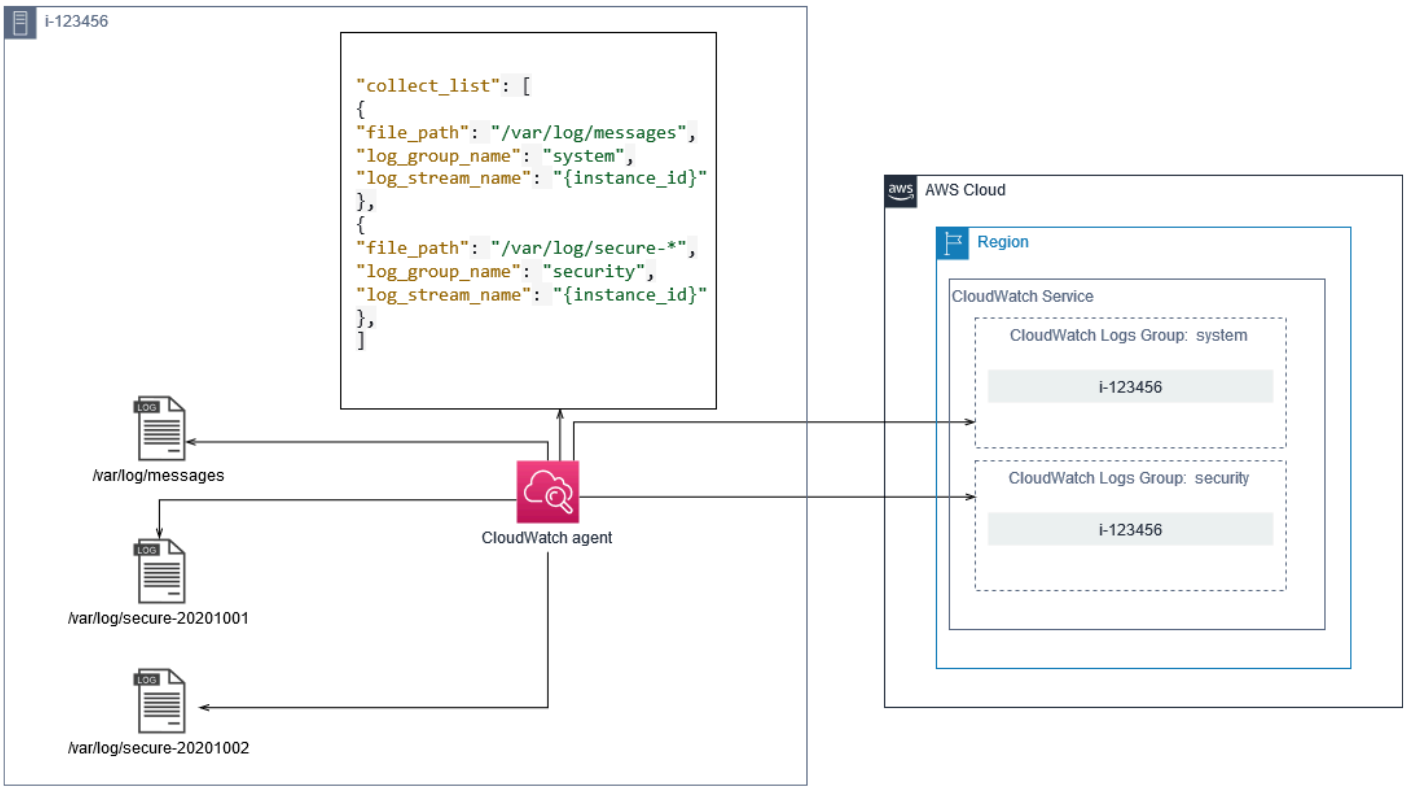
Por padrão, o Amazon EC2 não monitora nem captura arquivos de log. Em vez disso, os arquivos de log são capturados e ingeridos em CloudWatch Logs pelo CloudWatch Software de agente instalado na sua instância do EC2,AWSAPI ouAWS Command Line Interface(AWS CLI). Recomendamos usar o CloudWatch agente para ingerir arquivos de log em CloudWatch Logs do Amazon EC2 e servidores on-premises.

Você pode pesquisar e filtrar logs, bem como extrair métricas e executar automação com base em patches de padrões de arquivos de log no CloudWatch. CloudWatch oferece suporte a texto simples, delimitado por espaço e opções de sintaxe de padrão e filtro em formato JSON, com logs formatados em JSON proporcionando a maior flexibilidade. Para aumentar as opções de filtragem e análise, você deve usar uma saída de log formatada em vez de texto sem formatação.

O CloudWatch agent usa um arquivo de configuração que define os logs e as métricas para enviar ao CloudWatch. CloudWatch em seguida, captura cada arquivo de log como umStream de loge agrupa esses fluxos de log em umgrupo de log. Isso ajuda você a executar operações em logs de suas instâncias do EC2, como pesquisar por uma string correspondente.

O nome do fluxo de log padrão é o mesmo que o ID da instância do EC2 e o nome do grupo de logs padrão é o mesmo que o caminho do arquivo de log. O nome do fluxo de log deve ser exclusivo dentro do CloudWatch grupo de logs do Você pode usar `oinstance_id`,`hostname`,`local_hostname`, ou`ip_address`para substituição dinâmica no fluxo de log e nomes de grupos de logs, o que significa que você pode usar o mesmo CloudWatch O arquivo de configuração do agente em várias instâncias do EC2.

O seguinte diagrama mostra um CloudWatch configuração do agente para captura de logs. O grupo de logs é definido pelos arquivos de log capturados e contém fluxos de log separados para cada instância do EC2 porque o`{instance_id}`variável é usada para o nome do fluxo de log e as IDs de instância do EC2 são exclusivas.



Os grupos de log definem a retenção, as tags, a segurança, os filtros de métrica e o escopo de pesquisa para os fluxos de log que eles contêm. O comportamento de agrupamento padrão com base no nome do arquivo de log ajuda a pesquisar, criar métricas e alarmar dados específicos para um arquivo de log em instâncias do EC2 em uma conta e região. Você deve avaliar se o refinamento adicional do grupo de logs é necessário. Por exemplo, sua conta pode ser compartilhada por várias unidades de negócios e ter diferentes proprietários técnicos ou de operações. Isso significa que você deve refinar ainda mais o nome do grupo de logs para refletir a separação e a propriedade. Essa abordagem permite concentrar sua análise e solução de problemas na instância do EC2 relevante.

Se vários ambientes usarem uma conta, você poderá separar o registro para cargas de trabalho executadas em cada ambiente. A tabela a seguir mostra uma convenção de nomenclatura de grupos de logs que inclui a unidade de negócios, o projeto ou o aplicativo e o ambiente.

Nome do grupo de logs	`/<Business unit>/<Project or application name>/<Environment>/<Log file name>`

Nome do fluxo do log	`<EC2 instance ID>`

Você também pode agrupar todos os arquivos de log de uma instância do EC2 no mesmo grupo de logs. Isso facilita a pesquisa e a análise em um conjunto de arquivos de log para uma única instância do EC2. Isso é útil se a maioria das instâncias do EC2 atender a um aplicativo ou uma carga de trabalho e cada instância do EC2 atender a um propósito específico. A tabela a seguir mostra como o grupo de logs e a nomeação do fluxo de log podem ser formatados para dar suporte a essa abordagem.

Nome do grupo de logs	`/<Business unit>/<Project or application name>/<Environment>/<EC2 instance ID>`
Nome do fluxo do log	`<Log file name>`

Configurando a captura de métricas para instâncias do EC2

Por padrão, suas instâncias do EC2 estão habilitadas para monitoramento básico e umconjunto padrão de métricas(por exemplo, métricas relacionadas à CPU, rede ou armazenamento) são enviadas automaticamente para CloudWatch A cada cinco minutos. CloudWatch As métricas podem variar de acordo com a família da instância, por exemplo,Instâncias de desempenho intermitentestêm métricas para créditos de CPU. As métricas padrão do Amazon EC2 estão incluídas no preço da instância. Se você habilitar omonitoramento detalhadoPara suas instâncias do EC2, você pode receber dados em períodos de um minuto. A frequência do período afeta os custos do CloudWatch, portanto, verifique se o monitoramento detalhado é necessário para todas ou apenas algumas instâncias do EC2. Por exemplo, você pode habilitar o monitoramento detalhado para cargas de trabalho de produção, mas usar o monitoramento básico para cargas de trabalho que não são de produção.

Servidores locais não incluem métricas padrão para CloudWatch e deve usar o CloudWatch Agente do,AWS CLI, ouAWSSDK para capturar métricas. Isso significa que você deve definir as métricas que deseja capturar (por exemplo, utilização da CPU) na CloudWatch arquivo de configuração. Você pode criar um exclusivo CloudWatch arquivo de configuração que inclui as métricas de instância

padrão do EC2 para seus servidores locais e aplicá-lo além do padrão CloudWatch Configuração do .

Métricasem CloudWatch São definidas exclusivamente pelo nome da métrica e zero ou mais dimensões, e são agrupadas exclusivamente em um namespace de métricas. Métricas fornecidas por umAWSservice tem um namespace que começa com`AWS`(por exemplo,`AWS/EC2`), e não-AWSAs métricas são consideradas métricas personalizadas. Métricas que você configura e captura com o CloudWatch agente são todos considerados métricas personalizadas. Porque o número de métricas criadas afeta seu CloudWatch custos, você deve avaliar se cada métrica é necessária para todas ou apenas algumas de suas instâncias do EC2. Por exemplo, você poderia definir um conjunto completo de métricas para cargas de trabalho de produção, mas usar um subconjunto menor dessas métricas para cargas de trabalho que não sejam de produção.

`CWAgent`é o namespace padrão para métricas publicadas pelo CloudWatch Agente do. Semelhante aos grupos de logs, o namespace da métrica organiza um conjunto de métricas para que possam ser encontradas juntas em um só lugar. Você deve modificar o namespace para refletir uma unidade de negócios, projeto ou aplicativo e ambiente (por exemplo,`/<Business unit>/<Project or application name>/<Environment>`). Essa abordagem é útil se várias cargas de trabalho não relacionadas usarem a mesma conta. Você também pode correlacionar sua convenção de nomenclatura de namespace com sua CloudWatch convenção de nomeação de grupo de logs.

As métricas também são identificadas por suas dimensões, o que ajuda a analisá-las em relação a um conjunto de condições e são as propriedades nas quais as observações são registradas. O Amazon EC2 incluiMétricas separadaspara instâncias do EC2 com`InstanceId`e`AutoScalingGroupName`Dimensões. Você também recebe métricas com o`ImageId`e`InstanceType`Dimensões se você habilitar o monitoramento detalhado. Por exemplo, o Amazon EC2 fornece uma métrica de instância do EC2 separada para a utilização da CPU com o`InstanceId`dimensões, além de métrica de utilização de CPU separada para o`InstanceType`Dimensão do. Isso ajuda a analisar a utilização da CPU para cada instância exclusiva do EC2, além de todas as instâncias do EC2 de um específicotipo de instância.

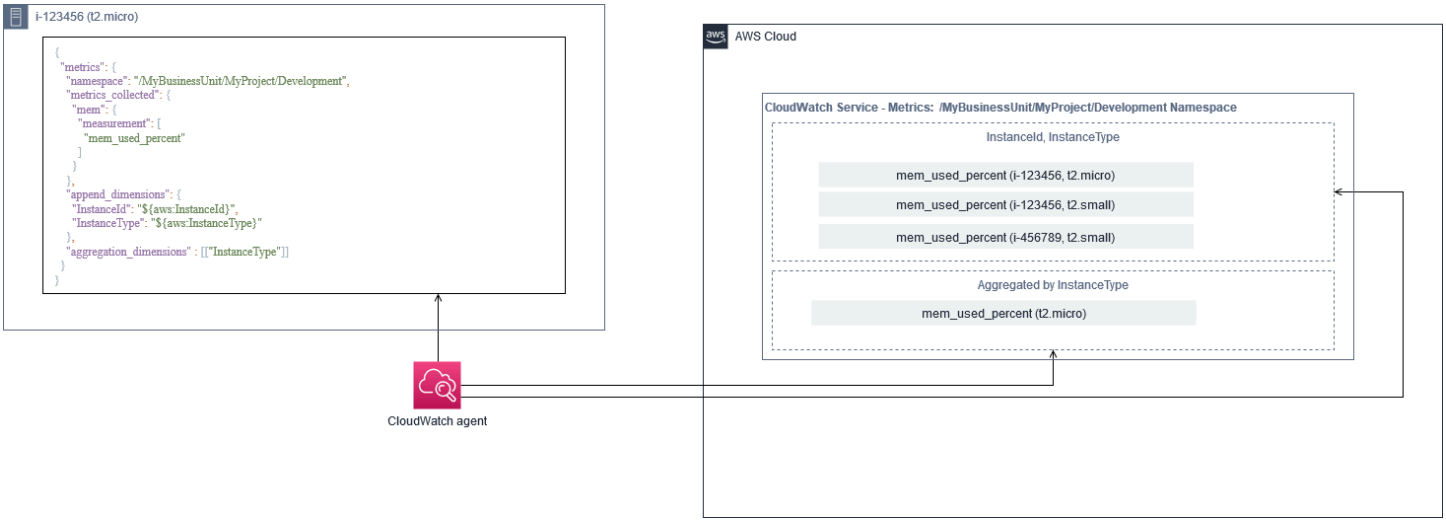
Adicionar mais dimensões aumenta sua capacidade de análise, mas também aumenta os custos gerais, porque cada métrica e combinação de valor de dimensão exclusiva resulta em uma nova métrica. Por exemplo, se você criar uma métrica para a porcentagem de utilização da memória em relação ao`InstanceId`dimensão, então esta é uma nova métrica para cada instância do EC2. Se sua organização executa milhares de instâncias do EC2, isso causará milhares de métricas e resulta em custos mais altos. Para controlar e prever custos, certifique-se de determinar a cardinalidade da métrica e quais dimensões adicionam mais valor. Por exemplo, você poderia definir um conjunto

completo de dimensões para as métricas de carga de trabalho de produção, mas um subconjunto menor dessas dimensões para cargas de trabalho que não sejam de produção.

Você pode usar o`append_dimensions`propriedade para adicionar dimensões a uma ou todas as métricas definidas em seu CloudWatch Configuração do . Você também pode anexar dinamicamente o`ImageId`,`InstanceId`,`InstanceType`, e`AutoScalingGroupName`para todas as métricas em seu CloudWatch Configuração do . Como alternativa, você pode acrescentar um nome e um valor de dimensão arbitrários para métricas específicas usando o`append_dimensions`propriedade nessa métrica. CloudWatch também pode agregar estatísticas sobre dimensões métricas que você definiu com o`aggregation_dimensions`propriedade.

Por exemplo, você pode agregar a memória usada contra o`InstanceType`dimensão para ver a memória média usada por todas as instâncias do EC2 para cada tipo de instância. Se você usar o`t2.micro`instâncias em execução em uma região, você poderia determinar se as cargas de trabalho usando o`t2.micro`classe estão utilizando demais ou subutilizando a memória fornecida. A subutilização pode ser um sinal de cargas de trabalho usando classes EC2 com capacidade de memória não necessária. Em contraste, a sobreutilização pode ser um sinal de cargas de trabalho usando classes do Amazon EC2 com memória insuficiente.

O diagrama a seguir mostra uma amostra CloudWatch configuração de métricas que usa um namespace personalizado, dimensões adicionadas e agregação por`InstanceType`.



Nível do sistema CloudWatch configuração

Métricas e registros no nível do sistema são um componente central de uma solução de monitoramento e registro, e o CloudWatch agent tem opções de configuração específicas para Windows e Linux.

Recomendamos usar oAssistente de arquivos de configuração do CloudWatchou esquema de arquivo de configuração para definir o CloudWatch arquivo de configuração do agente para cada sistema operacional que você planeja oferecer suporte. Registros e métricas adicionais específicos da carga de trabalho, no nível do SO podem ser definidos em separado CloudWatch arquivos de configuração e anexados à configuração padrão. Esses arquivos de configuração exclusivos devem ser armazenados separadamente em um bucket do S3, onde podem ser recuperados pelas instâncias do EC2. Um exemplo de uma configuração de bucket do S3 para essa finalidade é descrito naGerenciando CloudWatch configuraçõesSeção deste guia. Você pode recuperar e aplicar automaticamente essas configurações usando o State Manager and Distributor.

Configurar logs no nível do sistema

Os registros no nível do sistema são essenciais para diagnosticar e solucionar problemas no local ou noAWSNuvem. Sua abordagem de captura de log deve incluir todos os logs de sistema e segurança gerados pelo sistema operacional. Os arquivos de log gerados pelo sistema operacional podem ser diferentes, dependendo da versão do sistema operacional.

O CloudWatch o agente oferece suporte ao monitoramento de logs de eventos do Windows fornecendo o nome do log de eventos. Você pode escolher quais logs de eventos do Windows você deseja monitorar (por exemplo`System`,`Application`, ou`Security`).

Os logs de sistema, aplicativo e segurança para sistemas Linux geralmente são armazenados no`/var/log`Diretório. A tabela a seguir define os arquivos de log padrão comuns que você deve monitorar, mas você deve verificar o`/etc/rsyslog.conf`ou`/etc/syslog.conf`para determinar a configuração específica para os arquivos de log do sistema.

Distribuição do Fedora (Amazon Linux, CentOS, Red Hat Enterprise Linux)	`/var/log/boot.log*` — Registro de inicialização
	`/var/log/dmesg` — Log do Kernel

	`/var/log/secure` — Registro de segurança e autenticação
	`/var/log/messages` — Log geral do sistema
	`/var/log/cron*` — Cron Logs
	`/var/log/cloud-init-output.log` Saída do`Userdata`scripts de inicialização
Debian (Ubuntu)	`/var/log/syslog` — Registro de inicialização
	`/var/log/cloud-init-output.log` Saída do`Userdata`scripts de inicialização
	`/var/log/auth.log` — Registro de segurança e autenticação
	`/var/log/kern.log` — Log do Kernel

Sua organização também pode ter outros agentes ou componentes do sistema que geram logs que você deseja monitorar. Você deve avaliar e decidir quais arquivos de log são gerados por esses agentes ou aplicativos e incluí-los em sua configuração identificando a localização do arquivo. Por exemplo, você deve incluir o Systems Manager e CloudWatch registra o agente em sua configuração. A tabela a seguir fornece a localização desses logs de agente para Windows e Linux.

Windows	Agente do CloudWatch	`$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log`
	Agente Systems Manager	`%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log`

		`%PROGRAMDATA%\Amazon\SSM\Logs\errors.log`
		
		`%PROGRAMDATA%\Amazon\SSM\Logs\audits\amazon-ssm-agent-audit-YYYY-MM-DD`

Linux	Agente do CloudWatch	`/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log`

	Agente Systems Manager	`/var/log/amazon/ssm/amazon-ssm-agent.log`
		
		`/var/log/amazon/ssm/errors.log`
		
		`/var/log/amazon/ssm/audits/amazon-ssm-agent-audit-YYYY-MM-DD`

O CloudWatch ignora um arquivo de log se o arquivo de log estiver definido na CloudWatch configuração do agente, mas não foi encontrada. Isso é útil quando você deseja manter uma única configuração de log para Linux, em vez de configurações separadas para cada distribuição. Também é útil quando um arquivo de log não existe até que o agente ou o aplicativo de software comece a ser executado.

Configurar métricas no nível do sistema

A utilização de memória e espaço em disco não está incluída nas métricas padrão fornecidas pelo Amazon EC2. Para incluir essas métricas, você deve instalar e configurar o CloudWatch agente em suas instâncias do EC2. O CloudWatch O assistente de configuração do agente cria um CloudWatch Configuração com oMétricas predefinidas doE você pode adicionar ou remover métricas, conforme

necessário. Verifique os conjuntos de métricas predefinidos para determinar o nível apropriado necessário.

Os usuários finais e proprietários de cargas de trabalho devem publicar métricas adicionais do sistema com base em requisitos específicos para um servidor ou instância do EC2. Essas definições de métrica devem ser armazenadas, versionadas e mantidas em um separado CloudWatch arquivo de configuração do agente e compartilhado em um local central (por exemplo, Amazon S3) para reutilização e automação.

As métricas padrão do Amazon EC2 não são capturadas automaticamente em servidores locais. Essas métricas devem ser definidas em um CloudWatch arquivo de configuração do agente usado pelas instâncias locais. Você pode criar um arquivo de configuração de métrica separado para instâncias locais com métricas, como utilização da CPU, e ter essas métricas anexadas ao arquivo de configuração de métricas padrão.

Nível do aplicativo CloudWatch configuração

Os registros e as métricas de aplicativos são gerados pela execução de aplicativos e são específicos do aplicativo. Certifique-se de definir os logs e as métricas necessárias para monitorar adequadamente os aplicativos que são usados regularmente por sua organização. Por exemplo, sua organização pode ter padronizado no Microsoft Internet Information Server (IIS) para aplicativos baseados na Web. Você pode criar um log e uma métrica padrão CloudWatch configuração para o IIS que também pode ser usada em toda a organização. Os arquivos de configuração específicos do aplicativo podem ser armazenados em um local centralizado (por exemplo, um bucket do S3) e são acessados por proprietários de carga de trabalho ou por meio de recuperação automatizada e copiados para o CloudWatch Diretório de configuração. O CloudWatch agent combina automaticamente os arquivos de configuração do CloudWatch encontrados no diretório do arquivo de configuração de cada instância ou servidor do EC2 em um composto CloudWatch Configuração do . O resultado final é um CloudWatch configuração que inclui a configuração padrão no nível do sistema da sua organização, bem como todo o nível de aplicativo relevante CloudWatch configurações.

Os proprietários da carga de trabalho devem identificar e configurar arquivos de log e métricas para todos os aplicativos e componentes críticos.

Configurando logs no nível do aplicativo

O registro no nível do aplicativo varia dependendo se o aplicativo é comercial off-the-shelf (COTS) ou aplicativo desenvolvido sob medida. Os aplicativos COTS e seus componentes podem fornecer várias opções para configuração e saída de log, como nível de detalhes de log, formato de arquivo de log e localização do arquivo de log. No entanto, a maioria dos aplicativos COTS ou de terceiros não permite que você altere fundamentalmente o registro em log (por exemplo, atualizando o código do aplicativo para incluir instruções de log adicionais ou formatos que não são configuráveis). No mínimo, você deve configurar as opções de registro para COTS ou aplicativos de terceiros para registrar informações de aviso e de nível de erro, de preferência no formato JSON.

Você pode integrar aplicativos personalizados com CloudWatch Registros incluindo os arquivos de log do aplicativo em seu CloudWatch Configuração do . Aplicativos personalizados oferecem melhor qualidade e controle de log porque você pode personalizar o formato de saída de log, categorizar e separar a saída do componente para separar arquivos de log, além de incluir detalhes adicionais necessários. Certifique-se de revisar e padronizar as bibliotecas de log e os dados e formatação necessários para sua organização para que a análise e o processamento se tornem mais fáceis.

Você também pode escrever para um CloudWatch Stream de log com o CloudWatch Logs`PutLogEvents`Chamada de API ou usando oAWSSDK. Você pode usar a API ou o SDK para requisitos de log personalizados, como coordenar o registro em um único fluxo de log em um conjunto distribuído de componentes e servidores. No entanto, a solução mais fácil de manter e mais amplamente aplicável é configurar seus aplicativos para gravar em arquivos de log e, em seguida, usar o CloudWatch agente para ler e transmitir os arquivos de log para o CloudWatch.

Você também deve considerar o tipo de métricas que deseja medir a partir dos arquivos de log do aplicativo. Você pode usar filtros de métrica para medir, grafar e alarmar nesses dados em um CloudWatch grupo de logs do Por exemplo, você pode usar um filtro de métrica para contar tentativas de login com falha identificando-as em seus logs.

Você também pode criar métricas personalizadas para seus aplicativos personalizados usando o[Métrica incorporada do CloudWatchformatar](#)nos arquivos de log do aplicativo.

Configurar métricas no nível do aplicativo

Métricas personalizadas são métricas que não são fornecidas diretamente peloAWSserviços para o CloudWatch e eles são publicados em um namespace personalizado no CloudWatch Métricas do . Todas as métricas de aplicativos são consideradas personalizadas CloudWatch Métricas do . As métricas do aplicativo podem se alinhar a uma instância do EC2, componente de

aplicativo, chamada de API ou até mesmo uma função comercial. Você também deve considerar a importância e a cardinalidade das dimensões que você escolhe para suas métricas. Dimensões com alta cardinalidade geram um grande número de métricas personalizadas e podem aumentar sua CloudWatch da AWS.

O CloudWatch ajuda você a capturar métricas no nível do aplicativo de várias maneiras, incluindo as seguintes:

- Capture métricas em nível de processo definindo os processos individuais que você deseja capturar doplugin procstat.
- Um aplicativo publica uma métrica no Monitor de Desempenho do Windows e essa métrica é definida na CloudWatch Configuração do .
- Filtros e padrões métricos são aplicados em logs de um aplicativo no CloudWatch.
- Um aplicativo grava em um CloudWatch Log usando o CloudWatch formato de métrica incorporado.
- Um aplicativo envia uma métrica para CloudWatch Por meio da API ou daAWSSDK.
- Um aplicativo envia uma métrica para umcollectdouStatsDdaemon com um configurado CloudWatch Agente do.

Você pode usar procstat para monitorar e medir processos críticos de aplicativos com o agente do CloudWatch. Isso ajuda você a emitir um alarme e agir (por exemplo, uma notificação ou um processo de reinicialização) se um processo crítico não estiver mais em execução para o aplicativo. Você também pode medir as características de desempenho de seus processos de aplicação e emitir um alarme se um determinado processo estiver agindo de forma anormal.

O monitoramento Procstat também é útil se você não puder atualizar seus aplicativos COTS com métricas personalizadas adicionais. Por exemplo, você pode criar um`my_process`métrica que mede o`cpu_time`e inclui um personalizado`application_version`Dimensão do. Você também pode usar vários CloudWatch arquivos de configuração do agente para um aplicativo se você tiver dimensões diferentes para métricas diferentes.

Se o aplicativo for executado no Windows, você deverá avaliar se ele já publica métricas no Monitor de Desempenho do Windows. Muitos aplicativos COTS se integram ao Monitor de Desempenho do Windows, que ajuda você a monitorar facilmente as métricas de aplicativos. CloudWatch também se integra ao Monitor de Desempenho do Windows e você pode capturar todas as métricas que já estejam disponíveis nele.

Certifique-se de revisar o formato de registro e as informações de registro fornecidas por seus aplicativos para determinar quais métricas podem ser extraídas com filtros de métrica. Você pode revisar os registros históricos do aplicativo para determinar como as mensagens de erro e os desligamentos anormais são representados. Você também deve revisar os problemas relatados anteriormente para determinar se uma métrica pode ser capturada para evitar que o problema seja repetido. Você também deve revisar a documentação do aplicativo e pedir aos desenvolvedores de aplicativos que confirmem como as mensagens de erro podem ser identificadas.

Para aplicativos personalizados, trabalhe com os desenvolvedores do aplicativo para definir métricas importantes que podem ser implementadas usando o CloudWatch formato de métrica incorporado,AWSSDK ouAWSAPI. A abordagem recomendada é usar o formato de métricas incorporadas. Você pode usar oAWSforneceu bibliotecas de formato métrico incorporado de código aberto para ajudá-lo a escrever suas instruções no formato necessário. Você também precisa atualizar seuaplicativo específico do aplicativo CloudWatch configuraçãoPara incluir o agente de formato de métricas incorporadas. Isso faz com que o agente em execução na instância do EC2 atue como um endpoint de formato de métrica incorporado local que envia métricas de formato de métricas incorporadas ao CloudWatch.

Se seus aplicativos já suportam métricas de publicação para collectd ou statsd, você poderá aproveitá-los para ingerir métricas no CloudWatch.

Abordagens de instalação do agente CloudWatch para servidores Amazon EC2 e locais

Automatizar o CloudWatch o processo de instalação do agente ajuda você a implantá-lo de forma rápida e consistente e capturar os registros e métricas necessários. Existem várias abordagens para automatizar a instalação do agente CloudWatch, incluindo suporte a várias contas e várias regiões. As seguintes abordagens de instalação automatizada são discutidas:

- Instalar o CloudWatch agente usando o Systems Manager Distributor e o Systems Manager State Manager— Recomendamos usar essa abordagem se suas instâncias do EC2 e servidores locais estiverem executando o agente do Systems Manager. Isso garante que o CloudWatch o agente é mantido atualizado e você pode relatar e corrigir servidores que não têm o CloudWatch Agente. Essa abordagem também é dimensionada para oferecer suporte a várias contas e regiões.
- Implantar a CloudWatch agente como parte do script de dados do usuário durante o provisionamento de instâncias do EC2— O Amazon EC2 permite que você defina um script de inicialização que é executado quando você inicializa ou reinicializa pela primeira vez. Você pode definir um script para automatizar o processo de download e instalação do agente. Isso também pode ser incluído noAWS CloudFormationscripts eAWSProdutos do Service Catalog. Essa abordagem pode ser apropriada conforme necessário se houver uma abordagem personalizada de instalação e configuração do agente para uma carga de trabalho específica que se desvie de seus padrões.
- Incluir o agente do CloudWatch nas imagens de máquina da Amazon (AMIs)— Você pode instalar o agente do CloudWatch em suas AMIs personalizadas para o Amazon EC2. As instâncias do EC2 que usam a AMI terão automaticamente o agente instalado e iniciado. No entanto, você deve garantir que o agente e sua configuração sejam atualizados regularmente.

Instalar o CloudWatch Agente usando o Systems Manager Distributor e State Manager

Você pode usar o Systems Manager State Manager com o Systems Manager Distributor para instalar e atualizar automaticamente o CloudWatch agente em servidores e instâncias do EC2. O distribuidor inclui o`AmazonCloudWatchAgent` AWSpacote gerenciado que instala a versão mais recente do agente do CloudWatch.

Essa abordagem de instalação tem os seguintes pré-requisitos:

- O agente do Systems Manager deve ser instalado e executado nos servidores ou instâncias do EC2. O agente Systems Manager é pré-instalado no Amazon Linux, Amazon Linux 2 e algumas AMIs. O agente também deve ser instalado e configurado em outras imagens ou VMs e servidores locais.
- Uma função do IAM ou credenciais que têm orequeridos CloudWatch e permissões do Systems ManagerDevem ser anexados à instância do EC2 ou definidos no arquivo de credenciais de um servidor local. Por exemplo, você pode criar uma função do IAM que inclua oAWSpolíticas gerenciadas:`AmazonSSMManagedInstanceCore`Para Systems Manager e`CloudWatchAgentServerPolicy`para o CloudWatch. Você pode usar ossm-cloudwatch-instance-role.yaml AWS CloudFormationModelo para implantar uma função do IAM e um perfil de instância que inclui essas duas políticas. Esse modelo também pode ser modificado para incluir outras permissões padrão do IAM para suas instâncias do EC2. Para servidores locais ou VMs locais, deve configurar o CloudWatch Agente do para usar oFunção de serviço do Systems ManagerIsso foi configurado para o servidor local. Para obter mais informações sobre isso, consulteComo posso configurar servidores locais que usam o Systems Manager Agent e o unificado CloudWatch agente para usar apenas credenciais temporárias?noAWSCentral de conhecimento.

A lista a seguir fornece várias vantagens para usar a abordagem Systems Manager Distributor e State Manager para instalar e manter o CloudWatch Agente do:

- Instalação automatizada para vários sistemas operacionais— Você não precisa escrever e manter um script para cada sistema operacional para baixar e instalar o agente do CloudWatch.
- Verificações automáticas de atualização— O State Manager verifica automaticamente e regularmente se cada instância do EC2 tem a versão mais recente do CloudWatch.
- Relatórios de conformidade— O painel de conformidade do Systems Manager mostra quais instâncias do EC2 falharam ao instalar com êxito o pacote do distribuidor.
- Instalação automatizada para instâncias EC2 recém-lançadas— As novas instâncias do EC2 que são executadas em sua conta recebem automaticamente o CloudWatch Agente.

No entanto, você também deve considerar as três áreas a seguir antes de escolher essa abordagem:

- Colisão com uma associação existente— Se outra associação já instalar ou configurar o CloudWatch agente, então as duas associações podem interferir entre si e potencialmente causar

problemas. Ao usar essa abordagem, você deve remover todas as associações existentes que instalem ou atualizem o agente e a configuração do CloudWatch.

- Atualizar arquivos de configuração do agente personalizado— O distribuidor executa uma instalação usando o arquivo de configuração padrão. Se você usar um arquivo de configuração personalizado ou vários CloudWatch arquivos de configuração, você deve atualizar a configuração após a instalação.
- Configuração de várias regiões ou várias contas— A associação State Manager deve ser configurada em cada conta e região. Novas contas em um ambiente de várias contas devem ser atualizadas para incluir a associação do State Manager. Você precisa centralizar ou sincronizar o CloudWatch configuração para que várias contas e regiões possam recuperar e aplicar os padrões necessários.

Configurar o State Manager e o Distribuidor para CloudWatch implantação e configuração do agente

Você pode usarConfiguração rápida do Systems Managerpara configurar rapidamente os recursos do Systems Manager, incluindo a instalação e a atualização automática do CloudWatch agente em suas instâncias do EC2. A configuração rápida implanta umAWS CloudFormationpilha que implanta e configura os recursos do Systems Manager com base em suas escolhas.

A lista a seguir fornece duas ações importantes que são executadas pela Quick Setup para automatizado CloudWatch instalação e atualização do agente:

1. Criar documentos personalizados do Systems Manager— A Configuração rápida cria os seguintes documentos do Systems Manager para uso com o State Manager. Os nomes dos documentos podem variar, mas o conteúdo permanece o mesmo:
   - `CreateAndAttachIAMToInstance`— Cria o`AmazonSSMRoleForInstancesQuickSetup`perfil de função e instância se eles não existirem e anexar o`AmazonSSMManagedInstanceCore`Política do para a função. Isso não inclui o necessário`CloudWatchAgentServerPolicy`Política do IAM. Você deve atualizar essa política e atualizar este documento do Systems Manager para incluir essa política, conforme descrito na seção a seguir.
   - `InstallAndManageCloudWatchDocument`— Instala o CloudWatch agente com Distribuidor e configura cada instância do EC2 uma vez com um padrão CloudWatch Configuração do agente usando o`AWS-ConfigureAWSPackage`Documento do Systems Manager.

- `UpdateCloudWatchDocument`— Atualiza a CloudWatch Agente instalando o agente mais recente do CloudWatch usando o`AWS-ConfigureAWSPackage`Documento do Systems Manager. Atualizar ou desinstalar o agente não remove o existente CloudWatch Arquivos de configuração da instância do EC2.

2. Criar associações do State Manager— As associações do State Manager são criadas e configuradas para usar os documentos do Systems Manager criados personalizados. Os nomes de associação do State Manager podem variar, mas a configuração permanece a mesma:
   - `ManageCloudWatchAgent`— Executa `oInstallAndManageCloudWatchDocument`Documento do Systems Manager uma vez para cada instância do EC2.
   - `UpdateCloudWatchAgent`— Executa o`UpdateCloudWatchDocument`Documento do Systems Manager a cada 30 dias para cada instância do EC2.
   - Executa o`CreateAndAttachIAMToInstance`Documento do Systems Manager uma vez para cada instância do EC2.

Você deve aumentar e personalizar a configuração de Configuração rápida concluída para incluir permissões do CloudWatch e suporte personalizado CloudWatch configurações. Em particular, a`CreateAndAttachIAMToInstance`O e a`InstallAndManageCloudWatchDocument`documento precisará ser atualizado. Você pode atualizar manualmente os documentos do Systems Manager criados pela Quick Setup. Você também pode usar o seu CloudFormation modelo para provisionar os mesmos recursos com as atualizações necessárias, bem como configurar e implantar outros recursos do Systems Manager e não usar a Configuração rápida.

> **Important**
>
> A configuração rápida cria umAWS CloudFormationpilha para implantar e configurar recursos do Systems Manager com base em suas escolhas. Se você atualizar suas opções de Configuração rápida, talvez seja necessário reatualizar manualmente os documentos do Systems Manager.

As seções a seguir descrevem como atualizar manualmente os recursos do Systems Manager criados pela Quick Setup, bem como usar seus próprios AWS CloudFormationmodelo para executar

uma Configuração rápida atualizada. Recomendamos usar o seuAWS CloudFormationmodelo para evitar a atualização manual de recursos criados pela Quick Setup eAWS CloudFormation.

Use a Configuração Rápida do Systems Manager e atualize manualmente os recursos criados do Systems Manager

Os recursos do Systems Manager criados pela abordagem Quick Setup devem ser atualizados para incluir o necessário CloudWatch permissões de agente e suporte a vários CloudWatch Arquivos de configuração. Esta seção descreve como atualizar a função do IAM e os documentos do Systems Manager para usar um bucket centralizado do S3 contendo CloudWatch configurações acessíveis a partir de várias contas. Criar um bucket do S3 para armazenar o CloudWatch Os arquivos de configuração são discutidos noGerenciando CloudWatch configuraçõesSeção deste guia.

Atualizar o`CreateAndAttachIAMToInstance`Documento do Systems Manager

Este documento do Systems Manager criado pela Quick Setup verifica se uma instância do EC2 tem um perfil de instância do IAM existente anexado a ela. Se isso acontecer, ele anexa o`AmazonSSMManagedInstanceCore`Política para a função existente. Isso protege suas instâncias do EC2 existentes contra perdaAWSpermissões que podem ser atribuídas por meio de perfis de instância existentes. Você precisa adicionar uma etapa neste documento para anexar o`CloudWatchAgentServerPolicy`Política do IAM para instâncias do EC2 que já têm um perfil de instância anexado. O documento do Systems Manager também cria a função do IAM se ela não existir e uma instância do EC2 não tiver um perfil de instância anexado a ela. Você deve atualizar esta seção do documento para incluir também o`CloudWatchAgentServerPolicy`Política do IAM.

Analise o concluídoCreateAndAttachiamToInstance.YAMLexemplo de documento e compare com o documento criado pela Quick Setup. Edite o documento existente para incluir as etapas e alterações necessárias. Com base nas opções de Configuração rápida, o documento criado pela Quick Setup pode ser diferente do documento de amostra fornecido, portanto, certifique-se de fazer os ajustes necessários. O documento de exemplo inclui a opção Configuração rápida opção para verificar instâncias em busca de patches ausentes diariamente e, portanto, inclui uma política para o Systems Manager Patch Manager.

Atualizar o`InstallAndManageCloudWatchDocument`Documento do Systems Manager

Este documento do Systems Manager criado pela Quick Setup instala o CloudWatch agente e o configura com o padrão CloudWatch Configuração do agente. O valor CloudWatch a configuração

se alinha ao conjunto de métricas predefinido básico. Você deve substituir a etapa de configuração padrão e adicionar etapas para baixar o CloudWatch arquivos de configuração do seu CloudWatch configuração do bucket do S3.

Analise o concluídoInstallAndManageCloudWatchDocument.YAMLdocumento atualizado e compare-o com o documento criado pela Quick Setup. O documento criado pela Configuração rápida pode ser diferente, portanto, certifique-se de que você fez os ajustes necessários. Edite o documento existente para incluir as etapas e alterações necessárias.

Usar oAWS CloudFormationEm vez de Configuração rápida

Em vez de usar a configuração rápida da, você pode usarAWS CloudFormationpara configurar o Systems Manager. Essa abordagem permite que você personalize sua configuração do Systems Manager de acordo com suas necessidades específicas. Essa abordagem também evita atualizações manuais dos recursos configurados do Systems Manager criados pela Quick Setup para oferecer suporte personalizado CloudWatch configurações.

O recurso Configuração rápida também usaAWS CloudFormatione cria umAWS CloudFormationconjunto de pilha para implantar e configurar recursos do Systems Manager com base em suas escolhas. Antes que você possa usarAWS CloudFormationconjuntos de pilhas, é necessário criar as funções do IAM usadas porAWS CloudFormation StackSets para oferecer suporte a implantações em várias contas ou regiões. A Configuração rápida cria as funções necessárias para oferecer suporte a implantações em várias regiões ou várias contas comAWS CloudFormationStackSets. Você deve preencher os pré-requisitos doAWS CloudFormation StackSets se você quiser configurar e implantar recursos do Systems Manager em várias regiões ou várias contas a partir de uma única conta e região. Para obter mais informações sobre isso, consultePré-requisitos para operações de conjunto de pilhasnoAWS CloudFormationdocumentação.

Analise aAWS-QuickSetup-SSMHostMgmt.yaml AWS CloudFormationModelo para configuração rápida personalizada.

Você deve analisar os recursos e os recursos noAWS CloudFormationModelo e faça ajustes de acordo com suas necessidades. Você deve controlar a versãoAWS CloudFormationmodelo que você usa e teste incrementalmente as alterações para confirmar o resultado necessário. Além disso, você deve realizar revisões de segurança na nuvem para determinar se há algum ajuste de política necessário com base nos requisitos da sua organização.

Você deve implantar aAWS CloudFormationempilhe em uma única conta de teste e Região e execute todos os casos de teste necessários para personalizar e confirmar o resultado desejado. Em

seguida, você pode graduar sua implantação em várias regiões em uma única conta e, em seguida, para várias contas e várias regiões.

Configuração rápida personalizada em uma única conta e região com umAWS CloudFormationpilha

Se você estiver usando apenas uma única conta e Região, poderá implantar o exemplo completo como umAWS CloudFormationStack em vez de umAWS CloudFormationconjunto de pilhas. No entanto, se possível, recomendamos que você use a abordagem de conjunto de pilhas de várias contas e várias regiões, mesmo que use apenas uma única conta e região. O uso doAWS CloudFormation StackSets facilita a expansão para contas e regiões adicionais no future.

Use as etapas a seguir para implantar oAWS-QuickSetup-SSMHostMgmt.yaml AWS CloudFormationModelo como umAWS CloudFormationEmpilhar em uma única conta e região:

1. Faça o download do modelo e verifique-o em seu sistema de controle de versão preferido (por exemplo,AWS CodeCommit).
2. Personalize o padrãoAWS CloudFormationvalores de parâmetros com base nos requisitos da sua organização.
3. Personalizar as programações de associação do State Manager.
4. Personalizar o documento do Systems Manager com `aInstallAndManageCloudWatchDocument`ID lógico. Confirme se os prefixos de bucket do S3 se alinham aos prefixos para o bucket do S3 que contém o CloudWatch Configuração do .
5. Recuperar e registrar o nome de recurso da Amazon (ARN) do bucket do S3 que contém seu CloudWatch configurações. Para obter mais informações sobre isso, consulte aGerenciando CloudWatch configuraçõesSeção deste guia. Uma amostracloudwatch-config-s3-bucket.yaml AWS CloudFormationestá disponível um modelo que inclui uma política de bucket para fornecer acesso de leitura aoAWS Organizationscontas.
6. Implante a Configuração rápida personalizadaAWS CloudFormationModelo para a mesma conta do seu bucket do S3:
   - Para o`CloudWatchConfigBucketARN`, insira o ARN do bucket do S3.
   - Faça ajustes nas opções de parâmetros dependendo dos recursos que você deseja ativar para o Systems Manager.

7. Implante uma instância do EC2 de teste com e sem uma função do IAM para confirmar se a instância do EC2 funciona com o CloudWatch.

- Aplicar o`AttachIAMToInstance`Associação do State Manager. Este é um runbook do Systems Manager configurado para ser executado em um cronograma. As associações do State Manager que usam runbooks não são aplicadas automaticamente a novas instâncias do EC2 e podem ser configuradas para serem executadas de forma agendada. Para obter mais informações, consulteExecutar automações com acionadores usando o State ManagerNa documentação do Systems Manager.
- Confirme se a instância do EC2 tem a função do IAM necessária anexada.
- Confirme se o agente do Systems Manager está funcionando corretamente confirmando que a instância do EC2 está visível no Systems Manager.
- Confirmar que o CloudWatch agente está funcionando corretamente visualizando CloudWatch logs e métricas com base no CloudWatch Configurações do bucket do S3.

Configuração rápida personalizada em várias regiões e várias contas comAWS CloudFormationStackSets do

Se você estiver usando várias contas e regiões, poderá implantar oAWS-QuickSetup-SSMHostMgmt.yaml AWS CloudFormationmodelo como conjunto de pilhas. Você deve completar oAWS CloudFormationPré-requisitos do StackSetantes de usar conjuntos de pilhas. Os requisitos variam dependendo se você está implantando conjuntos de pilhas comauto-gerenciadoouGerenciado pelo serviçopermissões.

Recomendamos que você implante conjuntos de pilhas com permissões gerenciadas por serviço para que novas contas recebam automaticamente a Configuração rápida personalizada. Você deve implantar um conjunto de pilhas gerenciadas pelo serviço doAWS Organizationsconta de gerenciamento ou conta de administrador delegado. Você deve implantar o conjunto de pilhas a partir de uma conta centralizada usada para automação que tenha privilégios de administrador delegados, em vez deAWS Organizationsconta de gerenciamento. Também recomendamos que você teste a implantação do conjunto de pilhas direcionando uma unidade organizacional (UO) de teste com um único ou pequeno número de contas em uma região.

1. Conclua as etapas 1 a 5 doConfiguração rápida personalizada em uma única conta e região com umAWS CloudFormationpilhaSeção deste guia.

2. Faça login noAWS Management Console, abra aAWS CloudFormationconsoler e escolhaCriar StackSet:
   - SelecioneTemplate is ready (O modelo está pronto)eUpload a template file (Fazer upload de um arquivo de modelo). Carregar oAWS CloudFormationModelo que você personalizou de acordo com suas necessidades.
   - Especifique os detalhes do conjunto de pilhas:
     - Insira um nome de conjunto de pilhas, por exemplo,`StackSet-SSM-QuickSetup`.
     - Faça ajustes nas opções de parâmetros dependendo dos recursos que você deseja ativar para o Systems Manager.
     - Para o`CloudWatchConfigBucketARN`, insira o ARN do seu CloudWatch O bucket do S3 da configuração.
     - Especifique as opções do conjunto de pilhas, escolha se você usará permissões gerenciadas por serviço comAWS Organizationsou permissões autogerenciadas.
       - Se você escolher permissões autogerenciadas, insira oAWSCloudFormationStackSetAdministrationRoleeAWSCloudFormationStackSetExecutionRoleDe da função do IAM. A função de administrador deve existir na conta e a função de execução deve existir em cada conta de destino
   - para oGerenciado pelo serviçoPermissões comAWS OrganizationsRecomendamos que primeiro implante em uma UO de teste em vez de toda a organização.
     - Escolha se você deseja habilitar implantações automáticas. Recomendamos que você escolhaEnabled (Habilitado). Para o comportamento de remoção de conta, a configuração recomendada éExcluir pilhas.
   - para oauto-gerenciadopermissões, insira oAWSIDs de conta das contas que você quer configurar. Você deve repetir esse processo para cada nova conta se usar permissões autogerenciadas.
   - Insira as regiões onde você usará CloudWatch e do Systems Manager.
   - Confirme se a implantação foi bem-sucedida visualizando o status naOperações eInstâncias da pilhaguia para o conjunto de pilhas.
   - Teste esse Systems Manager e CloudWatch estão funcionando corretamente nas contas implantadas seguindo a etapa 7 da[Configuração rápida personalizada em uma única conta e região com umAWS CloudFormationpilha]Seção deste guia.

Considerações sobre como configurar servidores locais

O CloudWatch agente para servidores locais e VMs é instalado e configurado usando uma abordagem semelhante à das instâncias do EC2. No entanto, a tabela a seguir fornece considerações que você deve avaliar ao instalar e configurar o CloudWatch Agente em servidores no local e VMs locais.

Aponte a CloudWatch agente para as mesmas credenciais temporárias usadas para o Systems Manager.	Ao configurar o Systems Manager em um ambiente híbrido que inclui servidores locais, você pode ativar o Systems Manager com uma função do IAM. Você deve usar a função criada para suas instâncias do EC2 que inclui o `CloudWatchAgentServerPolicy` e `AmazonSSMManagedInstanceCore` políticas. Isso resulta no agente do Systems Manager recuperando e gravando credenciais temporárias em um arquivo de credenciais local. Você pode apontar seu CloudWatch configuração do agente para o mesmo arquivo. Você pode usar o processo de Configurar servidores locais que usam o agente Systems Manager e o agente unificado do CloudWatch para usar somente credenciais temporárias no AWSCentral de conhecimento. Você também pode automatizar esse processo definindo um runbook de automação do Systems Manager e uma associação do State Manager separados e segmentando suas instâncias locais com tags. Quando você cria um Ativação do Systems Manager para suas instâncias locais, você deve incluir uma tag que identifique as instâncias como instâncias locais.

Considere usar contas e regiões que tenham VPN ouAWS Direct ConnectAcesse eAWSPrivateLink.	Você pode usarAWS Direct ConnectouAWS Virtual Private Network(AWS VPN) Para estabelecer conexões privadas entre redes locais e sua nuvem privada virtual (VPC).AWS O PrivateLink estabelece uma conexão privada com CloudWatch Logs com um VPC endpoint de interface. Essa abordagem é útil se você tiver restrições que impedem que os dados sejam enviados pela Internet pública para um endpoint de serviço público.
Todas as métricas devem ser incluídas no CloudWatch Arquivo de configuração.	O Amazon EC2 inclui métricas padrão (por exemplo, utilização da CPU), mas essas métricas devem ser definidas para instâncias locais. Você pode usar um arquivo de configura ção de plataforma separado para definir essas métricas para servidores locais e, em seguida, anexar a configuração ao padrão CloudWatch configuração de métricas para a plataforma.

Considerações para instâncias efêmeras do EC2

As instâncias do EC2 são temporárias ouefêmeraSe forem provisionados pelo Auto Scaling do Amazon EC2, pelo Amazon EMR,Instâncias spot do Amazon EC2, ouAWS Batch. Instâncias efêmeras do EC2 podem causar um número muito grande de CloudWatch fluxos em um grupo de logs comum sem informações adicionais sobre sua origem de tempo de execução.

Se você usar instâncias efêmeras do EC2, considere adicionar informações contextuais dinâmicas adicionais no grupo de logs e nos nomes de fluxo de log. Por exemplo, você pode incluir o ID da solicitação de instância spot, o nome do cluster do Amazon EMR ou o nome do grupo Auto Scaling. Essas informações podem variar para instâncias EC2 recém-lançadas e talvez seja necessário recuperá-las e configurá-las em tempo de execução. Você pode fazer isso escrevendo um CloudWatch arquivo de configuração do agente na inicialização e reiniciando o agente para incluir o arquivo de configuração atualizado. Isso permite a entrega de logs e métricas para o CloudWatch usando informações dinâmicas de tempo de execução.

Você também deve se certificar de que suas métricas e registros sejam enviados pelo CloudWatch agente antes que suas instâncias efêmeras do EC2 sejam encerradas. O CloudWatch agente inclui um`flush_interval`parâmetro que pode ser configurado para definir o intervalo de tempo para o log de descarga e buffers métricos. Você pode diminuir esse valor com base em sua carga de trabalho e interromper o CloudWatch agente e force os buffers a serem liberados antes que a instância do EC2 seja encerrada.

Usando uma solução automatizada para implantar o CloudWatch agente

Se você usar uma solução de automação (por exemplo, Ansible ou Chef), poderá aproveitá-la para instalar e atualizar automaticamente o CloudWatch Agente. Se você usar essa abordagem, deverá avaliar as seguintes considerações:

- Valide se a automação cobre os sistemas operacionais e as versões do sistema operacional que você oferece suporte. Se o script de automação não suportar todos os sistemas operacionais da sua organização, você deve definir soluções alternativas para os sistemas operacionais sem suporte.
- Valide se a solução de automação verifica regularmente atualizações e atualizações do agente do CloudWatch. Sua solução de automação deve verificar regularmente se há atualizações para o CloudWatch agente ou desinstale e reinstale regularmente o agente. Você pode usar um agendador ou uma funcionalidade de solução de automação para verificar e atualizar regularmente o agente.
- Validar se você pode confirmar a conformidade com a instalação e a configuração do agente. Sua solução de automação deve permitir que você determine quando um sistema não tem o agente instalado ou quando o agente não está funcionando. Você pode implementar uma notificação ou um alarme em sua solução de automação para que as instalações e configurações com falha sejam rastreadas.

Implantar a CloudWatch agente durante o provisionamento de instâncias com o script de dados do usuário

Você pode usar essa abordagem se não planeja usar o Systems Manager e quiser usar seletivamente o CloudWatch para suas instâncias do EC2. Normalmente, essa abordagem é usada de uma só vez ou quando uma configuração especializada é necessária.AWSforneceLinks diretospara a CloudWatch agente que pode ser baixado em seus scripts de dados de inicialização ou usuário. Os pacotes de instalação do agente podem ser executados silenciosamente sem interação

do usuário, o que significa que você pode usá-los em implantações automatizadas. Se você usar essa abordagem, você deve avaliar as seguintes considerações:

- Maior risco de os usuários não instalarem o agente ou configurarem métricas padrão. Os usuários podem provisionar instâncias sem incluir as etapas necessárias para instalar o CloudWatch Agente. Eles também podem configurar incorretamente o agente, o que pode causar inconsistências de registro e monitoramento.
- Os scripts de instalação devem ser específicos do sistema operacional e adequados para diferentes versões do sistema operacional. Você precisa de scripts separados se você pretende usar o Windows e o Linux. O script Linux também deve ter diferentes etapas de instalação com base na distribuição.
- Você deve atualizar regularmente o CloudWatch agente com novas versões quando disponível. Isso pode ser automatizado se você usar o Systems Manager com o State Manager, mas também pode configurar o script de dados do usuário para executar novamente na inicialização da instância. O CloudWatch o agente é atualizado e reinstalado em cada reinicialização.
- Você deve automatizar a recuperação e a aplicação de configurações padrão do CloudWatch. Isso pode ser automatizado se você usar o Systems Manager com o State Manager, mas também pode configurar um script de dados do usuário para recuperar os arquivos de configuração na inicialização e reiniciar o CloudWatch Agente.

Incluir o CloudWatch agente em suas AMIs

A vantagem de usar essa abordagem é que você não precisa esperar pelo CloudWatch agente a ser instalado e configurado, e você pode iniciar imediatamente o registro e o monitoramento. Isso ajuda você a monitorar melhor as etapas de provisionamento e inicialização de instâncias caso as instâncias não sejam iniciadas. Essa abordagem também é apropriada se você não planeja usar o agente do Systems Manager. Se você usar essa abordagem, você deve avaliar as seguintes considerações:

- Um processo de atualização deve existir porque as AMIs podem não incluir as mais recentes CloudWatch Versão do agente do. O CloudWatch agente instalado em uma AMI só é atual até a última vez em que a AMI foi criada. Você deve incluir um método adicional para atualizar o agente regularmente e quando a instância do EC2 for provisionada. Se você usar o Systems Manager, poderá usar o[Instalar o CloudWatch Agente usando o Systems Manager Distributor e State Manager]Solução fornecida neste guia para isso. Se você não usar o Systems Manager,

poderá usar um script de dados do usuário para atualizar o agente na inicialização e reinicialização da instância.

- Suas CloudWatch o arquivo de configuração do agente deve ser recuperado na inicialização da instância. Se você não usar o Systems Manager, poderá configurar um script de dados do usuário para recuperar os arquivos de configuração na inicialização e, em seguida, reiniciar o CloudWatch Agente.
- O CloudWatch agente deve ser reiniciado após o seu CloudWatch A configuração é atualizada.
- AWScredenciais não devem ser salvas na AMI. Certifique-se de que nenhum localAWSAs credenciais são armazenadas na AMI. Se você usar o Amazon EC2, poderá aplicar a função do IAM necessária à sua instância e evitar credenciais locais. Se você usar instâncias locais, deverá automatizar ou atualizar manualmente as credenciais da instância antes de iniciar o CloudWatch Agente.

Registro e monitoramento no Amazon ECS

O Amazon Elastic Container Service (Amazon ECS) fornece dois tipos de lançamento para a execução de contêineres e que determinam o tipo de infraestrutura que hospeda tarefas e serviços; esses tipos de lançamento são o AWS Fargate Amazon EC2. Ambos os tipos de lançamento se integram CloudWatch , mas as configurações e o suporte variam.

As seções a seguir ajudam você a entender como usar CloudWatch o registro e o monitoramento no Amazon ECS.

Tópicos

- Configurando CloudWatch com um tipo de inicialização do EC2
- Registros de contêineres do Amazon ECS para os tipos de lançamento EC2 e Fargate
- Usando o roteamento de log personalizado com o Amazon FireLens ECS
- Métricas para o Amazon ECS

Configurando CloudWatch com um tipo de inicialização do EC2

Com um tipo de execução do EC2, você provisiona um cluster Amazon ECS de instâncias do EC2 que usam o CloudWatch agente para registro e monitoramento. Uma AMI otimizada do Amazon ECS vem pré-instalada com o agente de contêiner do Amazon ECS e fornece CloudWatch métricas para o cluster do Amazon ECS.

Essas métricas padrão estão incluídas no custo do Amazon ECS, mas a configuração padrão do Amazon ECS não monitora arquivos de log ou métricas adicionais (por exemplo, espaço livre em disco). Você pode usar o AWS Management Console para provisionar um cluster do Amazon ECS com o tipo de execução EC2. Isso cria uma AWS CloudFormation pilha que implanta um Amazon EC2 Auto Scaling grupo com uma configuração de execução. No entanto, essa abordagem significa que você não pode escolher uma AMI personalizada ou personalizar a configuração de execução com configurações diferentes ou scripts de inicialização adicionais.

Para monitorar registros e métricas adicionais, você deve instalar o CloudWatch agente em suas instâncias de contêiner do Amazon ECS. Você pode usar a abordagem de instalação para instâncias do EC2 na Instalar o CloudWatch Agente usando o Systems Manager Distributor e State Manager seção deste guia. No entanto, a AMI do Amazon ECS não inclui o agente necessário do Systems Manager. Você deve usar uma configuração de execução personalizada com um script de dados do

usuário que instala o agente do Systems Manager ao criar seu cluster Amazon ECS. Isso permite que suas instâncias de contêiner se registrem no Systems Manager e apliquem as associações do State Manager para instalar, configurar e atualizar o CloudWatch agente. Quando o State Manager executa e atualiza a configuração do seu CloudWatch agente, ele também aplica sua configuração padronizada em nível de sistema para o Amazon CloudWatch EC2. Você também pode armazenar CloudWatch configurações padronizadas para o Amazon ECS no bucket do S3 para sua CloudWatch configuração e aplicá-las automaticamente com o State Manager.

Você deve se certificar de que a função do IAM ou o perfil da instância aplicado às suas instâncias de contêiner do Amazon ECS incluam os requisitos `CloudWatchAgentServerPolicy` e `AmazonSSMManagedInstanceCore` as políticas. Você pode usar o modelo ecs_cluster_with_cloudwatch_linux.yaml para provisionar clusters Amazon AWS CloudFormation ECS baseados em Linux. Esse modelo cria um cluster do Amazon ECS com uma configuração de execução personalizada que instala o Systems Manager e implanta uma CloudWatch configuração personalizada para monitorar arquivos de log específicos do Amazon ECS.

Você deve capturar os seguintes registros para suas instâncias de contêiner do Amazon ECS, bem como seus registros de instância EC2 padrão:

- Resultado de inicialização do agente Amazon ECS — `/var/log/ecs/ecs-init.log`
- Saída do agente Amazon ECS — `/var/log/ecs/ecs-agent.log`
- Registro de solicitações do provedor de credenciais do IAM — `/var/log/ecs/audit.log`

Para obter mais informações sobre o nível de saída, a formatação e as opções adicionais de configuração, consulte os locais dos arquivos de log do Amazon ECS na documentação do Amazon ECS.

> **Important**
>
> A instalação ou configuração do agente não é necessária para o tipo de execução do Fargate porque você não executa nem gerencia instâncias de contêiner do EC2.

As instâncias de contêiner do Amazon ECS devem usar as AMIs otimizadas e o agente de contêiner mais recentes do Amazon ECS. AWS armazena parâmetros públicos do Systems Manager Parameter Store com informações de AMI otimizadas do Amazon ECS, incluindo o ID da AMI. Você pode recuperar a AMI otimizada mais recente do Parameter Store usando o formato de parâmetros

do Parameter Store para AMIs otimizadas do Amazon ECS. Você pode consultar o parâmetro público do Parameter Store que faz referência à AMI mais recente ou a uma versão específica da AMI em seus AWS CloudFormation modelos.

AWS fornece os mesmos parâmetros do Parameter Store em cada região suportada. Isso significa que os AWS CloudFormation modelos que fazem referência a esses parâmetros podem ser reutilizados em todas as regiões e contas sem que a AMI seja atualizada. Você pode controlar a implantação de novas AMIs do Amazon ECS em sua organização consultando uma versão específica, o que ajuda a evitar o uso de uma nova AMI otimizada do Amazon ECS até que você a teste.

Registros de contêineres do Amazon ECS para os tipos de lançamento EC2 e Fargate

O Amazon ECS usa uma definição de tarefa para implantar e gerenciar contêineres como tarefas e serviços. Você configura os contêineres que deseja iniciar em seu cluster Amazon ECS dentro de uma definição de tarefa. O registro é configurado com um driver de registro no nível do contêiner. Várias opções de drivers de log fornecem aos seus contêineres sistemas de registro diferentes (por exemplo,`awslogs`,`fluentd`,`gelf`,,`json-file`,`journald`,`logentries`,`splunk`, ou`awsfirelens`)`syslog`, dependendo se você usa o tipo de lançamento do EC2 ou do Fargate. O tipo de inicialização do Fargate fornece um subconjunto das seguintes opções de driver de log:`awslogs`,, e. `splunk` `awsfirelens` AWS fornece o driver de `awslogs` registro para capturar e transmitir a saída do contêiner para o CloudWatch Logs. As configurações do driver de registro permitem que você personalize o grupo de registros, a região e o prefixo do fluxo de registros junto com muitas outras opções.

A nomenclatura padrão para grupos de registros e a opção usada pela opção Configurar CloudWatch registros automaticamente no AWS Management Console é. `/ecs/<task_name>` O nome do stream de log usado pelo Amazon ECS tem o `<awslogs-stream-prefix>/<container_name>/<task_id>` formato. Recomendamos que você use um nome de grupo que agrupe seus registros com base nos requisitos da sua organização. Na tabela a seguir, os `image_name` e `image_tag` estão incluídos no nome do fluxo de log.

Nome do grupo de registros	`/<Business unit>/<Project or application name>/<Environment>/<Cluster name>/<Task name>`

Prefixo do nome do fluxo de log	`/<image_name>/<image_tag>`

Essas informações também estão disponíveis na definição da tarefa. No entanto, as tarefas são atualizadas regularmente com novas revisões, o que significa que a definição da tarefa pode ter sido usada de forma diferente `image_name` e `image_tag` diferente daquelas que a definição da tarefa está usando atualmente. Para obter mais informações e sugestões de nomes, consulte a Planejando sua CloudWatch implantação seção deste guia.

Se você usar um pipeline de integração contínua e entrega contínua (CI/CD) ou um processo automatizado, poderá criar uma nova revisão de definição de tarefa para seu aplicativo a cada nova criação de imagem do Docker. Por exemplo, você pode incluir o nome da imagem do Docker, a tag da imagem, a GitHub revisão ou outras informações importantes na definição da tarefa, na revisão e na configuração de registro como parte do processo de CI/CD.

Usando o roteamento de log personalizado com o Amazon FireLens ECS

FireLens for Amazon ECS, você pode rotear os registros para o Fluentd ou o FluentBit para que você possa enviar diretamente os registros de contêineres para AWS serviços e destinos da AWS Partner Network (APN), bem como oferecer suporte ao envio de registros para a Logs. CloudWatch

AWS fornece uma imagem Docker para o Fluent Bit com plug-ins pré-instalados para Amazon Kinesis Data Streams, Amazon Data Firehose e Logs. CloudWatch Você pode usar o driver de FireLens registro em vez do driver de `awslogs` registro para ter mais personalização e controle sobre os registros enviados para o CloudWatch Logs.

Por exemplo, você pode usar o driver de FireLens log para controlar a saída do formato de log. Isso significa que os CloudWatch logs de um contêiner do Amazon ECS são automaticamente formatados como objetos JSON e incluem propriedades formatadas em JSON para`ecs_cluster`,,, e. `ecs_task_arn` `ecs_task_definition` `container_id` `container_name` `ec2_instance_id` O host fluente é exposto ao seu contêiner por meio das variáveis de `FLUENT_PORT` ambiente `FLUENT_HOST` e quando você especifica o `awsfirelens` driver. Isso significa que você pode fazer login diretamente no roteador de log a partir do seu código usando bibliotecas de registradores fluentes. Por exemplo, seu aplicativo pode incluir a `fluent-logger-python` biblioteca para registrar no Fluent Bit usando os valores disponíveis nas variáveis de ambiente.

Se você optar FireLens por usar para o Amazon ECS, poderá definir as mesmas configurações do driver de `awslogs` log e usar outras configurações também. Por exemplo, você pode usar a definição de tarefa ecs-task-nginx-firelense.json do Amazon ECS que inicia um servidor NGINX configurado para ser usado para fazer login. FireLens CloudWatch Ele também lança um contêiner FireLens Fluent Bit como auxiliar para registro.

Métricas para o Amazon ECS

O Amazon ECS fornece CloudWatch métricas padrão (por exemplo, utilização de CPU e memória) para os tipos de lançamento do EC2 e do Fargate no cluster e no nível de serviço com o agente de contêiner do Amazon ECS. Você também pode capturar métricas para seus serviços, tarefas e contêineres usando o CloudWatch Container Insights ou capturar suas próprias métricas de contêiner personalizadas usando o formato métrico incorporado.

O Container Insights é um CloudWatch recurso que fornece métricas como utilização da CPU, utilização da memória, tráfego de rede e armazenamento nos níveis de cluster, instância de contêiner, serviço e tarefa. O Container Insights também cria painéis automáticos que ajudam você a analisar serviços e tarefas e ver a utilização média da memória ou da CPU no nível do contêiner. O Container Insights publica métricas `ECS/ContainerInsights` personalizadas no namespace personalizado que você pode usar para criar gráficos, alarmes e criar painéis.

Você pode ativar as métricas do Container Insight ativando o Container Insights para cada cluster individual do Amazon ECS. Se você também quiser ver métricas no nível da instância do contêiner, você pode iniciar o CloudWatch agente como um contêiner daemon no seu cluster do Amazon ECS. Você pode usar o AWS CloudFormation modelo cwagent-ecs-instance-metric-cfn.yaml para implantar o agente CloudWatch como um serviço do Amazon ECS. É importante ressaltar que esse exemplo pressupõe que você criou uma configuração de CloudWatch agente personalizada apropriada e a armazenou no Parameter Store com a chave`ecs-cwagent-daemon-service`.

O CloudWatchagente implantado como um contêiner daemon para o CloudWatch Container Insights inclui métricas adicionais de disco, memória e CPU, como `instance_cpu_reserved_capacity` e `instance_memory_reserved_capacity` com as dimensões`ClusterName`,`ContainerInstanceId`. `InstanceId` As métricas no nível da instância do contêiner são implementadas pelo Container Insights usando o formato métrico CloudWatch incorporado. Você pode configurar métricas adicionais em nível de sistema para suas instâncias de contêiner do Amazon ECS usando a abordagem da Configurar o State Manager e o Distribuidor para CloudWatch implantação e configuração do agente seção deste guia.

Criação de métricas de aplicativos personalizadas no Amazon ECS

Você pode criar métricas personalizadas para seus aplicativos usando o formato métrico CloudWatch incorporado. O driver de `awslogs` log pode interpretar declarações de formato métrico CloudWatch incorporado.

A variável de `CW_CONFIG_CONTENT` ambiente no exemplo a seguir é definida para o conteúdo do parâmetro `cwagentconfig` Systems Manager Parameter Store. Você pode executar o agente com essa configuração básica para configurá-lo como um endpoint de formato métrico incorporado. No entanto, isso não é mais necessário.

```
  {
  "logs": {
    "metrics_collected": {
      "emf": { }
    }
  }
}
```

Se você tiver implantações do Amazon ECS em várias contas e regiões, poderá usar um AWS Secrets Manager segredo para armazenar sua CloudWatch configuração e configurar a política secreta para compartilhá-la com sua organização. Você pode usar a opção secrets na definição da tarefa para definir a `CW_CONFIG_CONTENT` variável.

Você pode usar as bibliotecas de formato métrico incorporado de código aberto AWS fornecidas em seu aplicativo e especificar a variável de `AWS_EMF_AGENT_ENDPOINT` ambiente para se conectar ao contêiner auxiliar do CloudWatch agente, atuando como um endpoint de formato métrico incorporado. Por exemplo, você pode usar o aplicativo Python de amostra ecs_cw_emf_example para enviar métricas em formato métrico incorporado para um contêiner auxiliar do agente configurado como CloudWatch um endpoint de formato métrico incorporado.

O plug-in Fluent Bit para também CloudWatch pode ser usado para enviar mensagens de formato métrico incorporado. Você também pode usar o aplicativo Python de amostra ecs_firelense_emf_example para enviar métricas em formato métrico incorporado para um contêiner auxiliar Firelens for Amazon ECS.

Se você não quiser usar o formato métrico incorporado, você pode criar e atualizar CloudWatch métricas por meio da AWS API ou do AWS SDK. Não recomendamos essa abordagem, a menos

que você tenha um caso de uso específico, pois ela adiciona sobrecarga de manutenção e gerenciamento ao seu código.

Registro em log e monitoramento no Amazon EKS

O Amazon Elastic Kubernetes Service (Amazon EKS) integra-se ao CloudWatch Logs para o plano de controle do Kubernetes. O plano de controle é fornecido como um serviço gerenciado pelo Amazon EKS e você pode ativar o registro em log sem instalar um agente do CloudWatch. O CloudWatch o agente também pode ser implantado para capturar logs de nós e contêineres do Amazon EKS. Fluent Bit e Fluentd também são compatíveis com o envio de registros de contêiner para CloudWatch Logs.

O CloudWatch Container Insights fornece uma solução abrangente de monitoramento de métricas do Amazon EKS no nível de cluster, nó, pod, tarefa e serviço. O Amazon EKS também oferece suporte a várias opções para captura de métricas com Prometheus. O plano de controle do Amazon EKS fornece um endpoint de métricas O que expõe métricas em um formato do Prometheus. Você pode implantar o Prometheus em seu cluster do Amazon EKS para consumir essas métricas.

Você também pode Configurar a CloudWatch Agente para raspar métricas do Prometheus e crie CloudWatch métricas, além de consumir outros endpoints Prometheus. Monitoramento Container Insights para Prometheus também pode descobrir e capturar automaticamente métricas do Prometheus a partir de cargas de trabalho e sistemas compatíveis e em contêineres.

Você pode instalar e configurar o CloudWatch agente em seus nós do Amazon EKS, de forma semelhante à abordagem usada para o Amazon EC2 com o Distributor e o State Manager, para alinhar os nós do Amazon EKS com as configurações padrão de monitoramento e registro do sistema.

Registro em log para Amazon EKS

O registro em log do Kubernetes pode ser dividido em log do plano de controle, log de nós e registro de aplicativos. O Plano de controle do Kubernetes é um conjunto de componentes que gerenciam clusters do Kubernetes e produzem logs usados para fins de auditoria e diagnóstico. Com o Amazon EKS, você pode ativar logs para diferentes componentes do plano de controle e envie-os para o CloudWatch.

O Kubernetes também executa componentes do sistema, como `kubelet` e `kube-proxy` em cada nó do Kubernetes que executa seus pods. Esses componentes gravam logs em cada nó e você pode configurar CloudWatch e Container Insights para capturar esses logs para cada nó do Amazon EKS.

Os contêineres são agrupados comovagensdentro de um cluster do Kubernetes e estão programados para serem executados nos nós do Kubernetes. A maioria dos aplicativos em contêineres grava na saída padrão e no erro padrão, e o mecanismo de contêiner redireciona a saída para um driver de registro. No Kubernetes, os logs do contêiner são encontrados na`/var/log/pods`diretório em um nó. Você pode configurar o CloudWatch e Container Insights para capturar esses logs para cada um dos pods do Amazon EKS.

Registro em log do plano de controle do Amazon EKS

Um cluster do Amazon EKS consiste em um plano de controle de locatário único de alta disponibilidade para o cluster do Kubernetes e os nós do Amazon EKS que executam seus contêineres. Os nós do plano de controle são executados em uma conta gerenciada porAWS. Os nós de plano de controle de cluster do Amazon EKS são integrados com CloudWatch e você pode ativar o registro em log para componentes específicos do plano de controle.

Os registros são fornecidos para cada instância do componente do plano de controle do Kubernetes.AWSgerencia a integridade de seus nós de plano de controle e fornece umSLA (contrato de nível de serviço) para o endpoint Kubernetes.

Registro em log em nós e aplicativos do Amazon EKS

Recomendamos usar oCloudWatch Container Insightspara capturar registros e métricas para o Amazon EKS. O Container Insights implementa métricas em nível de cluster, nó e pod com o CloudWatch agente e Fluent Bit ou Fluentd para captura de log no CloudWatch. O Container Insights também fornece painéis automáticos com visualizações em camadas do seu capturado CloudWatch Métricas do . O Container Insights é implantado como CloudWatch DaemonSet e Fluent Bit DaemonSet que é executado em todos os nós do Amazon EKS. Os nós do Fargate não são suportados pelo Container Insights porque os nós são gerenciados porAWSe não oferece suporte a DaemonSets. O registro do Fargate para Amazon EKS é abordado separadamente neste guia.

A tabela a seguir mostra a CloudWatch grupos de log e logs capturados peloConfiguração padrão de captura de log Fluentd ou Fluent Bitpara o Amazon EKS.

`/aws/containerinsights/Cluster_Name/application`	Todos os arquivos de log em`/var/log/containers` . Este diretório fornece links simbólicos para todos os logs de contêiner do Kubernetes na`/var/log/pods` Estrutura de

	diretório do. Isso captura os registros do contêiner do aplicativo gravando em `stdout` ou `stderr`. Ele também inclui registros para contêineres do sistema Kubernetes, como `aws-vpc-cni-init`, `kube-proxy` e `coreDNS`.
`/aws/containerinsights/Cluster_Name/host`	Logs de `/var/log/dmesg`, `/var/log/secure` e `/var/log/messages`.
`/aws/containerinsights/Cluster_Name/dataplane`	Os logs no `/var/log/journal` para `kubelet.service`, `kubeproxy.service` e `docker.service`.

Se você não quiser usar o Container Insights com Fluent Bit ou Fluentd para registro em log, você pode capturar logs de nós e contêineres com o CloudWatch Agente instalado nos nós do Amazon EKS. Os nós do Amazon EKS são instâncias do EC2, o que significa que você deve incluí-las em sua abordagem de log padrão no nível do sistema para o Amazon EC2. Se você instalar o CloudWatch agente usando o Distribuidor e o State Manager, então os nós do Amazon EKS também estão incluídos no CloudWatch instalação, configuração e atualização do agente.

A tabela a seguir mostra logs específicos do Kubernetes e que você deve capturar se não estiver usando o Container Insights com Fluent Bit ou Fluentd para registro em log.

`/var/log/containers`	Este diretório fornece links simbólicos para todos os logs de contêiner do Kubernetes sob a `/var/log/pods` Estrutura de diretório do. Isso captura efetivamente os registros do contêiner do aplicativo gravando em `stdout` ou `stderr`. Isso inclui registros para contêineres do sistema Kubernetes, como `aws-vpc-cni-init`, `kube-proxy` e `coreDNS`. Importante: Isso não é necessário se você estiver usando o Container Insights.
`var/log/aws-routed-eni/ipamd.log`	Os logs do daemon L-IPAM podem ser encontrados aqui

`/var/log/aws-routed-eni/plugin.log`	

Você deve certificar-se de que os nós do Amazon EKS instalem e configurem o CloudWatch agente para enviar registros e métricas apropriadas no nível do sistema. No entanto, o AMI otimizado do Amazon EKS não inclui o agente do Systems Manager. Usar oModelos de execução, você pode automatizar a instalação do agente do Systems Manager e um padrão CloudWatch configuração que captura logs específicos importantes do Amazon EKS com um script de inicialização implementado por meio da seção de dados do usuário. Os nós do Amazon EKS são implantados usando um grupo Auto Scaling como umGrupo de nós gerenciadosou comoNós autogerenciados.

Com grupos de nós gerenciados, você fornece umModelo de execuçãoque inclui a seção de dados do usuário para automatizar a instalação do agente do Systems Manager e CloudWatch Configuração do . Você pode personalizar e usar oamazon_eks_managed_node_group_launch_config.yaml AWS CloudFormationmodelo para criar um modelo de execução que instala o agente do Systems Manager, CloudWatch agente, e também adiciona uma configuração de log específica do Amazon EKS ao CloudWatch Diretório de configuração. Este modelo pode ser usado para atualizar seu modelo de inicialização de grupos de nós gerenciados do Amazon EKS com um infrastructure-as-code (IaC) abordagem. Cada atualização para oAWS CloudFormationO modelo fornece uma nova versão do modelo de execução. Depois, você pode atualizar o grupo de nós para usar a nova versão do modelo e ter oProcesso de ciclo de vida gerenciadoatualize seus nós sem tempo de inatividade. Certifique-se de que a função do IAM e o perfil da instância aplicados ao grupo de nós gerenciados inclua o`CloudWatchAgentServerPolicy`e`AmazonSSMManagedInstanceCore` AWSpolíticas gerenciadas.

Com nós autogerenciados, você provisiona e gerencia diretamente o ciclo de vida e a estratégia de atualização para seus nós do Amazon EKS. Nós autogerenciados permitem executar nós do Windows em seu cluster do Amazon EKS eBottlerocket, junto comOutras opções. Você pode usarAWS CloudFormationpara implantar nós autogerenciados em seus clusters do Amazon EKS, o que significa que você pode usar uma abordagem de alteração gerenciada e iAC para seus clusters do Amazon EKS.AWSO fornece oamazon-eks-nodegroup.yaml AWS CloudFormationModelo que você pode usar no estado em que se encontram ou personalizar. O modelo provisiona todos os recursos necessários para nós do Amazon EKS em um cluster (por exemplo, uma função do IAM separada, grupo de segurança, grupo do Amazon EC2 Auto Scaling e um modelo de execução). Oamazon-eks-nodegroup.yaml AWS CloudFormationtemplate é uma versão atualizada que instala o

agente do Systems Manager necessário, CloudWatch agente, e também adiciona uma configuração de log específica do Amazon EKS ao CloudWatch Diretório de configuração.

Logging para Amazon EKS no Fargate

Com o Amazon EKS no Fargate, você pode implantar pods sem alocar ou gerenciar seus nós do Kubernetes. Isso elimina a necessidade de capturar logs no nível do sistema para os nós do Kubernetes. Para capturar os logs dos pods do Fargate, você pode usar o Fluent Bit para encaminhar os logs diretamente para o CloudWatch. Isso permite que você encaminhe registros automaticamente para CloudWatch sem configuração adicional ou um contêiner sidecar para seus pods do Amazon EKS no Fargate. Para obter mais informações sobre isso, consulteRegistro em log do Fargatena documentação do Amazon EKS eBit fluente para Amazon EKSnoAWSBlog. Esta solução captura o`STDOUT`e`STDERR`Streams de entrada/saída (E/S) do contêiner e os envia para CloudWatch por meio do Fluent Bit, com base na configuração Fluent Bit estabelecida para o cluster do Amazon EKS no Fargate.

Métricas para Amazon EKS e Kubernetes

O Kubernetes fornece uma API de métricas que permite acessar métricas de uso de recursos (por exemplo, uso de CPU e memória para nós e pods), mas a API fornece apenas informações point-in-time e não métricas históricas. OServidor de métricas Kubernetesnormalmente é usado para implantações do Amazon EKS e Kubernetes para agregar métricas, fornecer informações históricas de curto prazo sobre métricas e oferecer suporte a recursos comoHorizontal Pod Autoscaler.

O Amazon EKS expõe métricas de plano de controle por meio do servidor da API Kubernetesem um formato Prometheuse CloudWatch pode capturar e ingerir essas métricas. CloudWatch e o Container Insights também podem ser configurados para fornecer captura, análise e alarme de métricas abrangentes para os nós e pods do Amazon EKS.

Métricas do plano de controle do Kubernetes

O Kubernetes expõe métricas de plano de controle em um formato Prometheus usando o`/metrics`Endpoint da API HTTP. Você deve instalarPrometheusno cluster do Kubernetes para representar gráficos e visualizar essas métricas com um navegador da Web. Você também podeingerir as métricas expostaspelo servidor da API Kubernetes no CloudWatch.

Métricas de nó e sistema para Kubernetes

Kubernetes fornece o PrometheusServidor de métricaspod que você podeimplantar e executarem seus clusters do Kubernetes para estatísticas de memória e CPU em nível de cluster, nó e pod-level. Essas métricas são usadas com oHorizontal Pod AutoscalereVertical Pod Autoscaler. CloudWatch também pode fornecer essas métricas.

Você deve instalar o Kubernetes Metrics Server se você usar oPainel do Kubernetesou os autoescaladores horizontais e verticais. O Painel do Kubernetes ajuda você a navegar e configurar o cluster do Kubernetes, nós, pods e configuração relacionada, além de exibir as métricas de CPU e memória do Kubernetes Metrics Server. Você pode implantar essa solução para clusters individuais seguindo as etapas doImplantar o painel do Kubernetesna documentação do Amazon EKS.

As métricas fornecidas pelo Kubernetes Metrics Server não podem ser usadas para fins de não-auto scaling (por exemplo, monitoramento). As métricas são destinadas a point-in-time análise e não análise histórica. O painel do Kubernetes implanta o`dashboard-metrics-scraper`para armazenar métricas do Kubernetes Metrics Server por uma pequena janela de tempo.

O Container Insights usa uma versão em contêiner do CloudWatch agente que é executado em um Kubernetes DaemonSet para descobrir todos os contêineres em execução em um cluster e fornecer métricas no nível do nó. Ele coleta dados de desempenho em cada camada da pilha de desempenho. Você pode usar o Início rápido doAWSInício rápido ou configure o Container Insights separadamente. O Início rápido configura o monitoramento de métricas com a CloudWatch agente e registro em log com Fluent Bit para que você só precise implantá-lo uma vez para registro e monitoramento.

Como os nós do Amazon EKS são instâncias do EC2, você deve capturar métricas no nível do sistema, além das métricas capturadas pelo Container Insights, usando os padrões definidos para o Amazon EC2. Você pode usar a mesma abordagem doConfigurar o State Manager e o Distribuidor para CloudWatch implantação e configuração do agenteSeção deste guia para instalar e configurar o CloudWatch Agente para os clusters do Amazon EKS. Você pode atualizar seu arquivo de configuração específico do CloudWatch do Amazon EKS para incluir métricas, bem como a configuração de log específica do Amazon EKS.

O CloudWatch agente com suporte Prometheus pode descobrir e raspar automaticamente as métricas do Prometheus decargas de trabalho e sistemas compatíveis com contêineres. Ele os ingere como CloudWatch logs em formato métrico incorporado para análise com CloudWatch Registra o Insights e cria automaticamente métricas do CloudWatch.

> **Important**
>
> Você deveimplantar uma versão especializadado CloudWatch Agente para coletar métricas do Prometheus. Este é um agente separado do CloudWatch Agente implantado para o Container Insights. Você pode usar oprometheus_jmxaplicativo Java de exemplo, que inclui os arquivos de implantação e configuração para o CloudWatch agente e implantação de pod do Amazon EKS para demonstrar a descoberta de métricas do Prometheus. Para obter mais informações, consulteConfigurar amostra de workload do Java/JMX para o Amazon EKS e o Kubernetesna documentação do CloudWatch. Você também pode configurar o CloudWatch agente para capturar métricas de outros destinos do Prometheus em execução no cluster do Amazon EKS.

Métricas da aplicação

Você pode criar suas próprias métricas personalizadas com aFormato de métricas incorporadas ao CloudWatch. Para ingerir instruções de formato de métrica incorporadas, você precisa enviar entradas de formato de métrica incorporadas para um endpoint de formato de métrica incorporado. O CloudWatch agente pode ser configurado como umcontêiner sidecar no pod do Amazon EKS. O CloudWatch a configuração do agente é armazenada como um Kubernetes ConfigMap e leia por seu CloudWatch agent sidecar container para iniciar o endpoint de formato de métrica incorporado.

Você também pode configurar seu aplicativo como um destino do Prometheus e configurar o agente do CloudWatch, com suporte ao Prometheus, para descobrir, raspar e ingerir suas métricas no CloudWatch. Por exemplo, você pode usar aexportador JMX de código abertocom seus aplicativos Java para expor Beans JMX para consumo do Prometheus pelo CloudWatch Agente.

Se você não quiser usar o formato de métrica incorporado, também poderá criar e atualizar métricas do CloudWatch usandoAWSAPIouAWS SDK. No entanto, isso não é recomendável porque ela mistura o monitoramento e a lógica do aplicativo.

Métricas para o Amazon EKS no Fargate

O Fargate provisiona automaticamente nós do Amazon EKS para executar seus pods do Kubernetes para que você não precise monitorar e coletar métricas no nível do nó. No entanto, você deve monitorar métricas para pods em execução nos nós do Amazon EKS no Fargate. O Container Insights não está disponível no momento para o Amazon EKS no Fargate porque requer os seguintes recursos que não são suportados no momento:

- Atualmente, os DaemonSets não são compatíveis. O Container Insights é implantado executando o CloudWatch Agente do como um DaemonSet em cada nó de cluster.
- Não oferece suporte a volumes persistentes do HostPath. O CloudWatch o container do agente usa volumes persistentes do HostPath como um pré-requisito para a coleta de dados de métricas de contêiner.
- O Fargate impede contêineres privilegiados e acesso às informações do host.

Você pode usar oroteador de log integrado para FargatePara enviar instruções de formato de métricas incorporadas ao CloudWatch. O roteador de log usa Fluent Bit, que tem um CloudWatch plug-in que pode ser configurado para suportar instruções de formato métrico incorporadas.

Você pode recuperar e capturar métricas em nível de pod para seus nós do Fargate implantando o servidor Prometheus no cluster do Amazon EKS para coletar métricas dos nós do Fargate. Como o Prometheus requer armazenamento persistente, você pode implantar o Prometheus no Fargate se usar o Amazon Elastic File System (Amazon EFS) para armazenamento persistente. Você também pode implantar o Prometheus em um nó com suporte do Amazon EC2. Para obter mais informações, consulteComo monitorar o Amazon EKS noAWS Fargateusando Prometheus e GrafananoAWSBlog.

Monitoramento do Prometheus no Amazon EKS

Amazon Managed Service for Prometheusfornece um escalável, seguro,AWSserviço gerenciado para Prometheus de código aberto. Você pode usar o Prometheus query language (PromQL) para monitorar o desempenho de cargas de trabalho em contêiner sem gerenciar a infraestrutura subjacente para ingerir, armazenar e consultar métricas operacionais. Você pode coletar métricas do Prometheus do Amazon EKS e do Amazon ECS usandoAWSDistro for OpenTelemetry (ADOT)ou servidores Prometheus como agentes de coleta.

Monitoramento do CloudWatch Container Insights for Prometheuspermite que você configure e use o CloudWatch agente para descobrir métricas do Prometheus das cargas de trabalho do Amazon ECS, Amazon EKS e Kubernetes, e ingeri-las como métricas do CloudWatch. Esta solução é apropriada se CloudWatch é sua principal solução de observabilidade e monitoramento. No entanto, a lista a seguir descreve casos de uso em que o Amazon Managed Service for Prometheus oferece mais flexibilidade para ingerir, armazenar e consultar métricas do Prometheus:

- O Amazon Managed Service for Prometheus permite que você use servidores Prometheus existentes implantados no Amazon EKS ou Kubernetes autogerenciados e configure-os para gravar no Amazon Managed Service for Prometheus em vez de um armazenamento de dados configurado localmente. Isso remove o trabalho pesado indiferenciado do gerenciamento de um armazenamento de dados altamente disponível para seus servidores Prometheus e sua infraestrutura. O Amazon Managed Service for Prometheus é uma escolha adequada quando você tem uma implantação madura do Prometheus que deseja aproveitar noAWSNuvem.
- O Grafana suporta diretamente o Prometheus como fonte de dados para visualização. Se você quiser usar o Grafana com Prometheus em vez de CloudWatch Painéis para monitoramento de contêineres e, em seguida, o Amazon Managed Service for Prometheus pode atender às suas necessidades. O Amazon Managed Service for Prometheus integra-se ao Amazon Managed Grafana para fornecer uma solução gerenciada de monitoramento e visualização de código aberto.
- O Prometheus permite que você realize análises em suas métricas operacionais usando consultas do PromQL. Em contraste,a CloudWatch O agente ingere métricas do Prometheus no formato de métrica incorporadoem CloudWatch Registros que resultam em CloudWatch Métricas do . Você pode consultar os logs de formato de métricas incorporadas usando CloudWatch Logs Insights.
- Se você não planeja usar CloudWatch para monitoramento e captura de métricas, você deve usar o Amazon Managed Service for Prometheus com seu servidor Prometheus e uma solução de visualização, como o Grafana. Você precisa configurar seu servidor Prometheus para raspar métricas de seus destinos do Prometheus e configurar o servidor paraGravação remota no

seu espaço de trabalho do Amazon Managed Service for Prometheus. Se você usa o Amazon Managed Grafana, poderáintegre diretamente o Amazon Managed Grafana à sua fonte de dados do Amazon Managed Service for Prometheus usando o plug-in incluído. Como os dados métricos são armazenados no Amazon Managed Service for Prometheus, não há dependência para implantar o CloudWatch agente ou requisito para ingerir dados no CloudWatch. O CloudWatch O agente é necessário para o monitoramento do Container Insights for Prometheus.

Você também pode usar o ADOT Collector para extrair de um aplicativo instrumentado pelo Prometheus e enviar as métricas para o Amazon Managed Service for Prometheus. Para obter mais informações sobre o ADOT Collector, consulte oAWSDistro for OpenTelemetrydocumentação.

Registro e métricas paraAWS Lambda

Lambdaelimina a necessidade de gerenciar e monitorar servidores para suas cargas de trabalho e trabalha automaticamente com CloudWatchMétricas e CloudWatch Registra sem configuração ou instrumentação adicional do código do seu aplicativo. Esta seção ajuda você a entender as características de desempenho dos sistemas usados pelo Lambda e como suas escolhas de configuração influenciam o desempenho. Ele também ajuda você a registrar e monitorar suas funções do Lambda para otimizar o desempenho e diagnosticar problemas no nível do aplicativo.

Registro de funções Lambda

O Lambda transmite automaticamente a saída padrão e as mensagens de erro padrão de uma função do Lambda para CloudWatch Registros, sem a necessidade de drivers de registro. O Lambda também provisiona automaticamente contêineres que executam sua função Lambda e os configura para gerar mensagens de log em fluxos de log separados.

As invocações subsequentes da sua função do Lambda podem reutilizar o mesmo contêiner e a saída para o mesmo fluxo de log. O Lambda também pode provisionar um novo contêiner e enviar a invocação para um novo fluxo de log.

O Lambda cria automaticamente um grupo de registros quando sua função do Lambda é invocada pela primeira vez. As funções do Lambda podem ter várias versões e você pode escolher a versão que deseja executar. Todos os registros das invocações da função Lambda são armazenados no mesmo grupo de registros. O nome não pode ser alterado e está no`/aws/lambda/<YourLambdaFunctionName>`formato. Um fluxo de log separado é criado no grupo de logs para cada instância da função Lambda. O Lambda tem uma convenção de nomenclatura padrão para fluxos de log que usa um`YYYY/MM/DD/[<FunctionVersion>]<InstanceId>`formato. O`InstanceId`é gerado porAWSpara identificar a instância da função Lambda.

Recomendamos que você formate suas mensagens de log no formato JSON, pois você pode consultá-las mais facilmente com CloudWatch Informações sobre registros. Eles também podem ser filtrados e exportados com mais facilidade. Você pode usar uma biblioteca de registros para simplificar esse processo ou escrever suas próprias funções de manipulação de registros. Recomendamos que você use uma biblioteca de registros para ajudar a formatar e classificar as mensagens de registro. Por exemplo, se sua função Lambda estiver escrita em Python, você poderá usar oMódulo de registro em Pythonpara registrar mensagens e controlar o formato de saída. O Lambda usa nativamente a biblioteca de registro do Python para funções do Lambda escritas em

Python, e você pode recuperar e personalizar o registrador na sua função do Lambda.AWS O Labs criou oAWSLambda Powertools para Pythonkit de ferramentas para desenvolvedores para facilitar o enriquecimento de mensagens de log com dados importantes, como partidas a frio. O kit de ferramentas está disponível para Python, Java, Typescript e .NET.

Outra prática recomendada é definir o nível de saída do log usando uma variável e ajustá-la com base no ambiente e nos seus requisitos. O código da função do Lambda, além das bibliotecas usadas, pode gerar uma grande quantidade de dados de log, dependendo do nível de saída do log. Isso pode afetar seus custos de registro e afetar o desempenho.

O Lambda permite que você defina variáveis de ambiente para o ambiente de execução da função Lambda sem atualizar seu código. Por exemplo, você pode criar um`LAMBDA_LOG_LEVEL`variável de ambiente que define o nível de saída do log que você pode recuperar do seu código. O exemplo a seguir tenta recuperar um`LAMBDA_LOG_LEVEL`variável de ambiente e use o valor para definir a saída de registro. Se a variável de ambiente não estiver definida, o padrão será o`INFO`nível.

```
import logging
from os import getenv

logger = logging.getLogger()
log_level = getenv("LAMBDA_LOG_LEVEL", "INFO")
level = logging.getLevelName(log_level)
logger.setLevel(level)
```

Enviando registros para outros destinos de CloudWatch

Você pode enviar registros para outros destinos (por exemplo, Amazon). OpenSearch Serviço (ou função Lambda) usando filtros de assinatura. Se você não usa a Amazon OpenSearch Serviço, você pode usar uma função Lambda para processar os registros e enviá-los para umAWSserviço de sua escolha usando oAWSSDKs.

Você também pode usar SDKs para destinos de log fora doAWSUse a nuvem em sua função Lambda para enviar diretamente declarações de log para um destino de sua escolha. Se você escolher essa opção, recomendamos que considere o impacto da latência, do tempo adicional de processamento, do tratamento de erros e novas tentativas e do acoplamento da lógica operacional à sua função Lambda.

Métricas de função do Lambda

O Lambda permite que você execute seu código sem gerenciar ou escalar servidores, e isso quase elimina a carga de auditoria e diagnóstico em nível de sistema. No entanto, ainda é importante entender as métricas de desempenho e invocação no nível do sistema para suas funções do Lambda. Isso ajuda você a otimizar a configuração dos recursos e melhorar o desempenho do código. Monitorar e medir o desempenho de forma eficaz pode melhorar a experiência do usuário e reduzir seus custos ao dimensionar adequadamente suas funções do Lambda. Normalmente, as cargas de trabalho executadas como funções do Lambda também têm métricas em nível de aplicativo que precisam ser capturadas e analisadas. O Lambda suporta diretamente o formato métrico incorporado para tornar a captura em nível de aplicativo CloudWatch métricas mais fáceis.

Métricas em nível de sistema

O Lambda se integra automaticamente com CloudWatch Métricas e fornece um conjunto demétricas padrão para suas funções do Lambda. O Lambda também fornece um painel de monitoramento separado para cada função do Lambda com essas métricas. Duas métricas importantes que você precisa monitorar são erros e erros de invocação. Entender as diferenças entre erros de invocação e outros tipos de erro ajuda você a diagnosticar e oferecer suporte às implantações do Lambda.

Erros de invocaçãoevite que sua função Lambda seja executada. Esses erros ocorrem antes da execução do código, portanto, você não pode implementar o tratamento de erros no código para identificá-los. Em vez disso, você deve configurar alarmes para suas funções do Lambda que detectem esses erros e notifiquem as operações e os proprietários da carga de trabalho. Esses erros geralmente estão relacionados a um erro de configuração ou permissão e podem ocorrer devido a uma alteração na configuração ou nas permissões. Os erros de invocação podem iniciar uma nova tentativa, o que causa várias invocações da sua função.

Uma função Lambda invocada com sucesso retorna uma resposta HTTP 200 mesmo que uma exceção seja lançada pela função. Suas funções do Lambda devem implementar o tratamento de erros e gerar exceções para que o`Errors`a métrica captura e identifica execuções com falha da sua função Lambda. Você deve retornar uma resposta formatada de suas invocações de função do Lambda que inclua informações para determinar se a execução falhou completamente, parcialmente ou foi bem-sucedida.

CloudWatch forneceCloudWatch Insights do Lambdaque você pode ativar para funções individuais do Lambda. O Lambda Insights coleta, agrega e resume métricas em nível de sistema (por exemplo,

tempo de CPU, memória, disco e uso da rede). O Lambda Insights também coleta, agrega e resume informações de diagnóstico (por exemplo, partidas a frio e desligamentos de funcionários do Lambda) para ajudá-lo a isolar e resolver problemas rapidamente.

O Lambda Insights usa o formato métrico incorporado para emitir automaticamente informações de desempenho para o`/aws/lambda-insights/`grupo de registros com um prefixo de nome de fluxo de registros baseado no nome da sua função do Lambda. Esses eventos de registro de desempenho criam CloudWatch métricas que são a base da automação CloudWatch painéis. Recomendamos que você habilite o Lambda Insights para testes de desempenho e ambientes de produção. Métricas adicionais criadas pelo Lambda Insights incluem`memory_utilization`isso ajuda a dimensionar corretamente as funções do Lambda para que você evite pagar por capacidade não necessária.

Métricas da aplicação

Você também pode criar e capturar suas próprias métricas de aplicativo no CloudWatch usando o formato métrico incorporado. Você pode aproveitarBibliotecas fornecidas pela AWS para formato métrico incorporadopara criar e emitir declarações de formato métrico incorporado para CloudWatch. O Lambda integrado CloudWatch o recurso de registro está configurado para processar e extrair instruções de formato métrico incorporado formatadas adequadamente.

Pesquisando e analisando registros CloudWatch

Depois que seus registros e métricas forem capturados em um formato e local consistentes, você poderá pesquisá-los e analisá-los para ajudar a melhorar a eficiência operacional, além de identificar e solucionar problemas. Recomendamos que você capture seus registros em um formato bem formado (por exemplo, JSON) para facilitar a pesquisa e a análise de seus registros. A maioria das cargas de trabalho usa uma coleção deAWS recursos, como rede, computação, armazenamento e bancos de dados. Sempre que possível, você deve analisar coletivamente as métricas e os registros desses recursos e correlacioná-los para monitorar e gerenciar com eficácia todas as suasAWS cargas de trabalho.

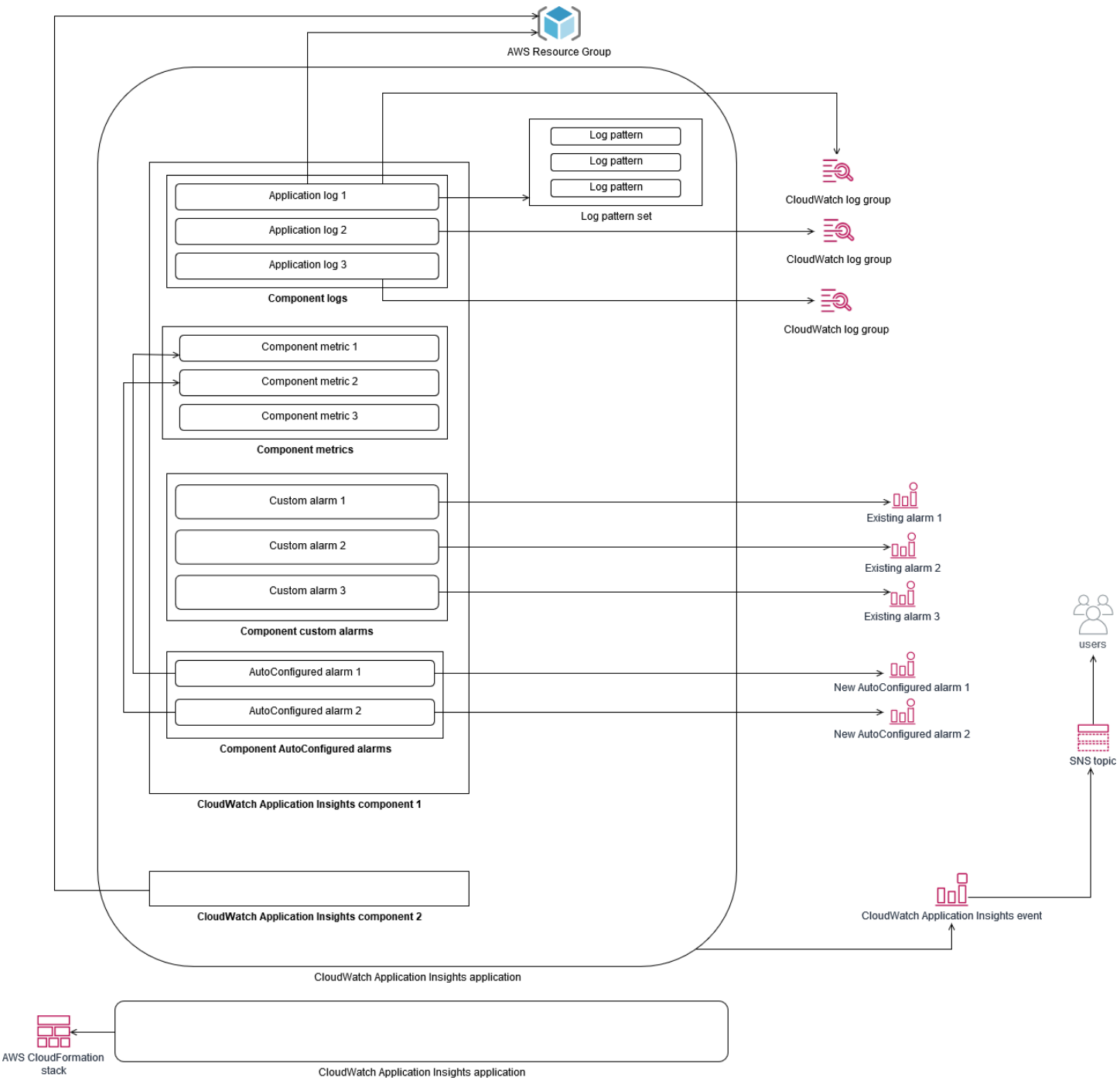
CloudWatch fornece vários recursos para ajudar a analisar registros e métricas, como o CloudWatch Application Insights para definir e monitorar coletivamente métricas e registros de um aplicativo em diferentesAWS recursos e a detecção de anomalias na superfície de seuCloudWatch métricas e CloudWatch Log Insights para pesquisar e analisar dados de log de modo interativo no CloudWatch Logs.

Monitore e analise coletivamente os aplicativos com o CloudWatch Application Insights

Os proprietários de aplicativos podem usar o Amazon CloudWatch Application Insights para configurar o monitoramento e a análise automáticos de cargas de trabalho. Isso pode ser configurado além do monitoramento padrão em nível de sistema configurado para todas as cargas de trabalho em uma conta. Configurar o monitoramento por meio do CloudWatch Application Insights também pode ajudar as equipes de aplicativos a se alinharem proativamente às operações e reduzir o tempo médio de recuperação (MTTR). CloudWatch O Application Insights pode ajudar a reduzir o esforço necessário para estabelecer registros e monitoramento em nível de aplicativo. Ele também fornece uma estrutura baseada em componentes que ajuda as equipes a dividir as responsabilidades de registro e monitoramento.

CloudWatch O Application Insights usa grupos de recursos para identificar os recursos que devem ser monitorados coletivamente como um aplicativo. Os recursos suportados no grupo de recursos se tornam componentes definidos individualmente do seu CloudWatch aplicativo Application Insights. Cada componente do seu CloudWatch aplicativo Application Insights tem seus próprios registros, métricas e alarmes.

Para registros, você define o conjunto de padrões de log que deve ser usado para o componente e dentro do seu CloudWatch aplicativo Application Insights. Um conjunto de padrões de log é uma coleção de padrões de log a serem pesquisados com base em expressões regulares, junto com uma severidade baixa, média ou alta para quando o padrão é detectado. Para métricas, você escolhe as métricas a serem monitoradas para cada componente em uma lista de métricas compatíveis e específicas do serviço. Para alarmes, o CloudWatch Application Insights cria e configura automaticamente alarmes padrão ou de detecção de anomalias para as métricas que estão sendo monitoradas. CloudWatch O Application Insights tem configurações automáticas para métricas e captura de registros para as tecnologias descritas nos registros e métricas suportadas pelo CloudWatch Application Insights na CloudWatch documentação. O diagrama a seguir mostra as relações entre os componentes do CloudWatch Application Insights e suas configurações de registro e monitoramento. Cada componente definiu seus próprios registros e métricas para monitorar usando CloudWatch registros e métricas.



As instâncias do EC2 monitoradas pelo CloudWatch Application Insights exigem o Systems Manager, CloudWatch agentes e permissões. Para obter mais informações sobre isso, consulte Pré-requisitos para configurar um CloudWatch aplicativo com o Application Insights na CloudWatch documentação. CloudWatch O Application Insights usa o Systems Manager para instalar e atualizar o CloudWatch agente. As métricas e os registros configurados no CloudWatch Application Insights criam um arquivo de configuração do CloudWatch agente que é armazenado em um parâmetro do Systems

Manager com o`AmazonCloudWatch-ApplicationInsights-SSMParameter` prefixo de cada componente do CloudWatch Application Insights. Isso resulta na adição de um arquivo de configuração de CloudWatch agente separado ao diretório de configuração do CloudWatch agente na instância do EC2. Um comando do Systems Manager é executado para acrescentar essa configuração à configuração ativa na instância do EC2. CloudWatch O uso do Application Insights não afeta as configurações existentes do CloudWatch agente. Você pode usar o CloudWatch Application Insights além de suas próprias configurações de sistema e CloudWatch agente em nível de aplicativo. No entanto, você deve garantir que as configurações não se sobreponham.

Realizando análise de registros com o CloudWatch Logs Insights

CloudWatch O Logs Insights facilita a pesquisa de vários grupos de registros usando uma linguagem de consulta simples. Se os registros do seu aplicativo estiverem estruturados no formato JSON, o CloudWatch Logs Insights descobrirá automaticamente os campos JSON em seus fluxos de log em vários grupos de registros. Você pode usar o CloudWatch Logs Insights para analisar os registros do aplicativo e do sistema, o que salva suas consultas para uso future. A sintaxe de consulta do CloudWatch Logs Insights oferece suporte a funções como agregação com funções, por exemplo, sum (), avg (), count (), min () e max (), que podem ser úteis para solucionar problemas de aplicativos ou análise de desempenho.

Se você usar o formato de métrica incorporado para criar CloudWatch métricas, poderá consultar seus registros de formato métrico incorporado para gerar métricas únicas usando as funções de agregação suportadas. Isso ajuda a reduzir seus custos de CloudWatch monitoramento ao capturar os pontos de dados necessários para gerar métricas específicas conforme necessário, em vez de capturá-las ativamente como métricas personalizadas. Isso é especialmente eficaz para dimensões com alta cardinalidade que resultariam em um grande número de métricas. CloudWatch O Container Insights também adota essa abordagem e captura dados detalhados de desempenho, mas gera CloudWatch métricas apenas para um subconjunto desses dados.

Por exemplo, a seguinte entrada de métrica incorporada gera somente um conjunto limitado de CloudWatch métricas a partir dos dados métricos capturados na declaração de formato de métrica incorporada:

```
{
 "AutoScalingGroupName": "eks-e0bab7f4-fa6c-64ba-dbd9-094aee6cf9ba",
 "CloudWatchMetrics": [
 {
 "Metrics": [
```

```
{
"Unit": "Count",
"Name": "pod_number_of_container_restarts"
}
],
"Dimensions": [
[
"PodName",
"Namespace",
"ClusterName"
]
],
"Namespace": "ContainerInsights"
}
],
"ClusterName": "eksdemo",
"InstanceId": "i-03b21a16b854aa4ca",
"InstanceType": "t3.medium",
"Namespace": "amazon-cloudwatch",
"NodeName": "ip-172-31-10-211.ec2.internal",
"PodName": "cloudwatch-agent",
"Sources": [
"cadvisor",
"pod",
"calculated"
],
"Timestamp": "1605111338968",
"Type": "Pod",
"Version": "0",
"pod_cpu_limit": 200,
"pod_cpu_request": 200,
"pod_cpu_reserved_capacity": 10,
"pod_cpu_usage_system": 3.268605094109382,
"pod_cpu_usage_total": 8.899539221131045,
"pod_cpu_usage_user": 4.160042847048305,
"pod_cpu_utilization": 0.44497696105655227,
"pod_cpu_utilization_over_pod_limit": 4.4497696105655224,
"pod_memory_cache": 4096,
"pod_memory_failcnt": 0,
"pod_memory_hierarchical_pgfault": 0,
"pod_memory_hierarchical_pgmajfault": 0,
"pod_memory_limit": 209715200,
"pod_memory_mapped_file": 0,
```

```
 "pod_memory_max_usage": 43024384,
 "pod_memory_pgfault": 0,
 "pod_memory_pgmajfault": 0,
 "pod_memory_request": 209715200,
 "pod_memory_reserved_capacity": 5.148439982463127,
 "pod_memory_rss": 38481920,
 "pod_memory_swap": 0,
 "pod_memory_usage": 42803200,
 "pod_memory_utilization": 0.6172094650851303,
 "pod_memory_utilization_over_pod_limit": 11.98828125,
 "pod_memory_working_set": 25141248,
 "pod_network_rx_bytes": 3566.4174629544723,
 "pod_network_rx_dropped": 0,
 "pod_network_rx_errors": 0,
 "pod_network_rx_packets": 3.3495665260575094,
 "pod_network_total_bytes": 4283.442421354973,
 "pod_network_tx_bytes": 717.0249584005006,
 "pod_network_tx_dropped": 0,
 "pod_network_tx_errors": 0,
 "pod_network_tx_packets": 2.6964010534762948,
 "pod_number_of_container_restarts": 0,
 "pod_number_of_containers": 1,
 "pod_number_of_running_containers": 1,
 "pod_status": "Running"
}
```


No entanto, você pode consultar as métricas capturadas para obter mais informações. Por exemplo, você pode executar a seguinte consulta para ver os 20 pods mais recentes com falhas na página de memória:

```
fields @timestamp, @message
| filter (pod_memory_pgfault > 0)
| sort @timestamp desc
| limit 20
```

Realizando análise de registros com o Amazon OpenSearch Service

CloudWatch integra-se com o Amazon OpenSearch Service, permitindo que você transmita dados de CloudWatch log de grupos de log para um cluster do Amazon OpenSearch Service de sua

escolha com um filtro de assinatura. Você pode usar CloudWatch para captura e análise primárias de registros e métricas e, em seguida, aumentá-los com o Amazon OpenSearch Service para os seguintes casos de uso:

- Controle refinado de acesso a dados — O Amazon OpenSearch Service permite que você limite o acesso aos dados até o nível do campo e ajuda a tornar os dados anônimos nos campos com base nas permissões do usuário. Isso é útil se você quiser oferecer suporte à solução de problemas sem expor dados confidenciais.
- Agregue e pesquise registros em várias contas, regiões e infraestrutura — Você pode transmitir seus registros de várias contas e regiões para um cluster comum do Amazon OpenSearch Service. Suas equipes de operações centralizadas podem analisar tendências, problemas e realizar análises em todas as contas e regiões. O streaming de CloudWatch registros para o Amazon OpenSearch Service também ajuda você a pesquisar e analisar um aplicativo multirregional em um local central.
- Envie e enriqueça registros diretamente para o Amazon OpenSearch Service usando ElasticSearch agentes — Seus componentes de aplicativos e pilhas de tecnologia podem usar sistemas operacionais que não são suportados pelo CloudWatch agente. Talvez você também queira enriquecer e transformar os dados de registro antes que eles sejam enviados para sua solução de registro. O Amazon OpenSearch Service oferece suporte a clientes padrão do Elasticsearch, como os remetentes de dados da família Elastic Beats e o Logstash, que oferecem suporte ao enriquecimento e à transformação de registros antes de enviar os dados de log para o Amazon OpenSearch Service.
- A solução de gerenciamento de operações existente usa umaElasticSearch pilha Logstash, Kibana (ELK) para registro e monitoramento — talvez você já tenha um investimento significativo no Amazon OpenSearch Service ou no Elasticsearch de código aberto com muitas cargas de trabalho já configuradas. Você também pode ter painéis operacionais criados no Kibana e que você deseja continuar a usar.

Se você não planeja usar CloudWatch registros, pode usar agentes, drivers de log e bibliotecas compatíveis com o Amazon OpenSearch Service (por exemplo, Fluent Bit, Fluentd, logstash e Open Distro for ElasticSearch API) para enviar seus registros diretamente para o Amazon OpenSearch Service e ignorá-los CloudWatch. No entanto, você também deve implementar uma solução para capturar registros gerados pelosAWS serviços. CloudWatch O Logs é a principal solução de captura de registros para muitosAWS serviços e vários serviços criam automaticamente novos grupos de registros CloudWatch. Por exemplo, o Lambda cria um novo grupo de registros para cada função

do Lambda. Você pode configurar um filtro de assinatura para que um grupo de registros transmita seus registros para o Amazon OpenSearch Service. Você pode configurar manualmente um filtro de assinatura para cada grupo de log individual que você deseja transmitir para o Amazon OpenSearch Service. Como alternativa, você pode implantar uma solução que inscreva automaticamente novos grupos de registros em ElasticSearch clusters. Você pode transmitir registros para um ElasticSearch cluster na mesma conta ou em uma conta centralizada. O streaming de registros para um ElasticSearch cluster na mesma conta ajuda os proprietários da carga de trabalho a analisar e dar suporte melhor às cargas de trabalho.

Você deve considerar a configuração de um ElasticSearch cluster em uma conta centralizada ou compartilhada para agregar registros em suas contas, regiões e aplicativos. Por exemplo,AWS Control Tower configura uma conta do Log Archive que é usada para registro centralizado. Quando uma nova conta é criada noAWS Control Tower, seusAWS Config registrosAWS CloudTrail e registros são entregues a um bucket do S3 nessa conta centralizada. O registro instrumentado peloAWS Control Tower é para registro de configuração, alteração e auditoria.

Para estabelecer uma solução centralizada de análise de registros de aplicativos com o Amazon OpenSearch Service, você pode implantar um ou mais clusters centralizados do Amazon OpenSearch Service em sua conta de registro centralizada e configurar grupos de registros em suas outras contas para transmitir registros para o Amazon OpenSearch Service centralizado. clusters.

Você pode criar clusters separados do Amazon OpenSearch Service para lidar com diferentes aplicativos ou camadas de sua arquitetura de nuvem que podem ser distribuídos em suas contas. O uso OpenSearch de clusters separados do Amazon Service ajuda a reduzir o risco de segurança e disponibilidade, e ter um cluster comum do Amazon OpenSearch Service pode facilitar a pesquisa e a relação de dados dentro do mesmo cluster.

Opções alarmantes com o CloudWatch

A realização de análises únicas e automatizadas de métricas importantes ajuda a detectar e resolver problemas antes que eles afetem suas cargas de trabalho. CloudWatch facilita o gráfico e a comparação de várias métricas usando várias estatísticas em um período de tempo específico. Você pode usar CloudWatch para pesquisar em todas as métricas com os valores de dimensão necessários para encontrar as métricas necessárias para sua análise.

Recomendamos que você comece sua abordagem de captura de métricas, incluindo um conjunto inicial de métricas e dimensões para usar como linha de base para monitorar uma carga de trabalho. Com o tempo, a carga de trabalho amadurece e você pode adicionar métricas e dimensões adicionais para ajudá-lo a analisar e dar suporte a ela. Seus aplicativos ou cargas de trabalho podem usar váriosAWSrecursos e ter suas próprias métricas personalizadas, você deve agrupar esses recursos em um namespace para torná-los mais fáceis de identificar.

Você também deve considerar como os dados de registro e monitoramento são correlacionados para que você possa identificar rapidamente os dados relevantes de registro e monitoramento para diagnosticar problemas específicos. Você pode usarCloudWatch ServiceLenspara correlacionar vestígios, métricas, registros e alarmes para diagnosticar problemas. Você também deve considerar a inclusão de dimensões adicionais em métricas e identificadores em logs para suas cargas de trabalho para ajudá-lo a pesquisar e identificar problemas rapidamente entre sistemas e serviços.

O uso do CloudWatch Alarmes para monitorar e alarmar

Você pode usarAlarmes do CloudWatchpara reduzir o monitoramento manual em suas cargas de trabalho ou aplicativos. Você deve começar revisando as métricas que você está capturando para cada componente de carga de trabalho e determinar os limites apropriados para cada métrica. Certifique-se de identificar quais membros da equipe devem ser notificados quando um limite for violado. Você deve estabelecer e direcionar grupos de distribuição, em vez de membros individuais da equipe.

Os alarmes do CloudWatch podem se integrar à sua solução de gerenciamento de serviços para criar automaticamente novos tickets e executar fluxos de trabalho operacionais. Por exemplo,AWSFornece oAWSConector de gerenciamento de serviços paraServiceNoweService Desk do JiraPara ajudá-lo a configurar rapidamente integrações. Essa abordagem é fundamental para garantir que os alarmes levantados sejam reconhecidos e alinhados aos fluxos de trabalho de operações existentes que já possam estar definidos nesses produtos.

Você também pode criar vários alarmes para a mesma métrica que tem diferentes limites e períodos de avaliação, o que ajuda a estabelecer um processo de escalonamento. Por exemplo, se tiver um`OrderQueueDepth`métrica que rastreia pedidos de clientes, você pode definir um limite mais baixo em um curto período médio de um minuto que notifica os membros da equipe de aplicativos por e-mail ouSlack. Você também pode definir outro alarme para a mesma métrica em um período mais longo de 15 minutos no mesmo limite e que páginas, e-mails e notifica o líder da equipe de aplicativos e da equipe de aplicativos. Finalmente, você pode definir um terceiro alarme para um limite médio difícil durante um período de 30 minutos que notifica o gerenciamento superior e notifica todos os membros da equipe notificados anteriormente. A criação de vários alarmes ajuda você a tomar ações diferentes para condições diferentes. Você pode começar com um processo de notificação simples e, em seguida, ajustá-lo e melhorá-lo conforme necessário.

O uso do CloudWatch detecção de anomalias para monitorar e alarmar

Você pode usarDetecção de anomalias do CloudWatchse você não tiver certeza sobre os limites a serem aplicados a uma determinada métrica ou se quiser que um alarme ajuste automaticamente os valores de limite com base em valores históricos observados. CloudWatch a detecção de anomalias é particularmente útil para métricas que podem ter mudanças regulares e previsíveis na atividade, por exemplo, pedidos de compra diários para entrega no mesmo dia aumentando antes de um tempo limite. A detecção de anomalias permite limites que se ajustam automaticamente e podem ajudar a reduzir alarmes falsos. Você pode habilitar a detecção de anomalias para cada métrica e estatística e configurar CloudWatch para alarme com base em outliers.

Por exemplo, você pode habilitar a detecção de anomalias para o`CPUUtilization`Métrica do e`AVG`Estatística em uma instância do EC2. A detecção de anomalias usa até 14 dias de dados históricos para criar o modelo de aprendizado de máquina (ML). Você pode criar vários alarmes com diferentes faixas de detecção de anomalias para estabelecer um processo de escalonamento de alarme, semelhante à criação de vários alarmes padrão com diferentes limites.

Para obter mais informações sobre essa seção, consulteCriar um alarme do CloudWatch com base na detecção de anomaliasno CloudWatch documentação.

Alarmante em várias regiões e contas

Os proprietários de aplicativos e cargas de trabalho devem criar alarmes no nível do aplicativo para cargas de trabalho que abrangem várias regiões. Recomendamos criar alarmes separados em cada

conta e região em que sua carga de trabalho é implantada. Você pode simplificar e automatizar esse processo usando conta e região independenteAWS CloudFormation StackSets e modelos para implantar recursos de aplicativos com os alarmes necessários. TemplateVocê pode configurar as ações de alarme para direcionar um tópico comum do Amazon Simple Notification Service (Amazon SNS), o que significa que a mesma ação de notificação ou correção é usada independentemente da conta ou região.

Em ambientes com várias contas e várias regiões, recomendamos que você crie alarmes agregados para suas contas e regiões para monitorar problemas de conta e regionais usandoAWS CloudFormation StackSets e métricas agregadas, como média`CPUUtilization`Em todas as instâncias do EC2.

Você também deve considerar a criação de alarmes padrão para cada carga de trabalho configurada para o padrão CloudWatch métricas e registros que você captura. Por exemplo, você pode criar um alarme separado para cada instância do EC2 que monitora a métrica de utilização da CPU e notifica uma equipe de operações central quando a utilização média da CPU for superior a 80% diariamente. Você também pode criar um alarme padrão que monitora a utilização média da CPU abaixo de 10% diariamente. Esses alarmes ajudam a equipe de operações centrais a trabalhar com proprietários de carga de trabalho específicos para alterar o tamanho das instâncias do EC2 quando necessário.

Automatizar a criação de alarmes com tags de instâncias do EC2

A criação de um conjunto padrão de alarmes para suas instâncias do EC2 pode ser demorado, inconsistente e propenso a erros. Você pode acelerar o processo de criação de alarme usando oalarmes automáticos amazon-cloudwatch-solução para criar automaticamente um conjunto padrão de alarmes do CloudWatch para suas instâncias do EC2 e criar alarmes personalizados com base em tags de instância do EC2. A solução elimina a necessidade de criar alarmes padrão manualmente e pode ser útil durante uma migração em larga escala de instâncias do EC2 que usa ferramentas como o CloudEndure. Você também pode implantar essa solução comAWS CloudFormation StackSets Para oferecer suporte a várias regiões e contas. Para obter mais informações, consulteUsar tags para criar e manter a Amazon CloudWatch Alarmes para instâncias do Amazon EC2noAWSBlog.

Monitoramento da disponibilidade de aplicativos e serviços

O CloudWatch ajuda você a monitorar e analisar os aspectos de desempenho e tempo de execução de seus aplicativos e cargas de trabalho. Você também deve monitorar os aspectos de disponibilidade e acessibilidade de seus aplicativos e cargas de trabalho. É possível fazer isso usando uma abordagem de monitoramento ativa comVerificações de integridade do Amazon Route 53eCloudWatch Synthetics.

Você pode usar as verificações de integridade do Route 53 quando quiser monitorar a conectividade com uma página da Web por meio de HTTP ou HTTPS ou conectividade de rede por meio de TCP para um nome ou endereço IP público do Sistema de Nomes de Domínio (DNS). As verificações de integridade do Route 53 iniciam conexões das Regiões especificadas em intervalos de dez segundos ou 30 segundos. Você pode escolher várias Regiões para que a verificação de integridade seja executada, cada verificação de integridade é executada de forma independente e você deve escolher pelo menos três Regiões. Você pode pesquisar o corpo da resposta de uma solicitação HTTP ou HTTPS para uma substring específica se ela aparecer nos primeiros 5.120 bytes de dados retornados para avaliação de verificação de integridade. Uma solicitação HTTP ou HTTPS é considerada íntegra se retornar uma resposta 2xx ou 3xx. As verificações de integridade do Route 53 podem ser usadas para criar uma verificação de integridade composta, verificando a integridade de outras verificações de saúde. Você pode fazer isso se você tiver vários endpoints de serviço e quiser executar a mesma notificação quando um deles não estiver íntegro. Se você usar o Route 53 para DNS, poderá configurar o Route 53 parafailover para outra entrada DNSse uma verificação de saúde se tornar insalubre. Para cada carga de trabalho crítica, você deve considerar configurar verificações de integridade do Route 53 para endpoints externos essenciais para operações normais. As verificações de integridade do Route 53 podem ajudá-lo a evitar gravar lógica de failover em seus aplicativos.

Os sintéticos do CloudWatch permitem que você defina um canário como um script para avaliar a integridade e a disponibilidade de suas cargas de trabalho. Canaries são scripts escritos em Node.js ou Python e funcionam em protocolos HTTP ou HTTPS. Eles criam funções do Lambda em sua conta que usam Node.js ou Python como framework. Cada canário definido pode executar várias chamadas HTTP ou HTTPS para endpoints diferentes. Isso significa que você pode monitorar a integridade de uma série de etapas, como um caso de uso ou um endpoint com dependências downstream. Canaries criam CloudWatch métricas que incluem cada etapa executada para que você possa alarmar e medir diferentes etapas de forma independente. Embora os canários exijam mais planejamento e esforço para serem desenvolvidos do que as verificações de integridade do

Route 53, elas fornecem uma abordagem de monitoramento e avaliação altamente personalizável. Os Canaries também oferecem suporte a recursos privados executados em sua nuvem privada virtual (VPC), o que os torna ideais para monitoramento de disponibilidade quando você não tem um endereço IP público para o endpoint. Você também pode usar canais para monitorar cargas de trabalho locais, desde que você tenha conectividade de dentro da VPC para o endpoint. Isso é particularmente importante quando você tem uma carga de trabalho que inclui endpoints existentes no local.

Aplicações de rastreamento comAWS X-Ray

Uma solicitação por meio de seu aplicativo pode consistir em chamadas para bancos de dados, aplicativos e serviços da Web em execução em servidores locais, Amazon EC2, contêineres ou Lambda. Ao implementar o rastreamento de aplicativos, você pode identificar rapidamente a causa raiz dos problemas em seus aplicativos que usam componentes e serviços distribuídos. É possível usar oAWS X-Raypara rastrear suas solicitações de aplicativos em vários componentes. Amostras de X-Ray e visualiza solicitações em umGráfico de serviçoquando eles fluem pelos componentes do aplicativo e cada componente é representado como um segmento. O X-Ray gera identificadores de rastreamento para que você possa correlacionar uma solicitação quando ela flui por vários componentes, o que ajuda a visualizar a solicitação de ponta a ponta. Você pode aprimorar ainda mais isso, incluindo anotações e metadados para ajudar a pesquisar e identificar exclusivamente as características de uma solicitação.

Recomendamos que você configure e instrumente cada servidor ou endpoint em seu aplicativo com o X-Ray. O X-Ray é implementado no código do aplicativo fazendo chamadas para o serviço X-Ray. O X-Ray também forneceAWSSDKs para vários idiomas, incluindo clientes instrumentados que enviam dados automaticamente para o X-Ray. Os SDKs do X-Ray fornecem patches para bibliotecas comuns usadas para fazer chamadas para outros serviços (por exemplo, HTTP, MySQL, PostgreSQL ou MongoDB).

O X-Ray fornece um daemon X-Ray que você pode instalar e executar no Amazon EC2 e no Amazon ECS para retransmitir dados para o X-Ray. O X-Ray cria rastreamentos para o aplicativo que capturam dados de desempenho dos servidores e contêineres que executam o daemon X-Ray que atendeu a solicitação. O X-Ray ajusta automaticamente suas chamadas paraAWSserviços, como o Amazon DynamoDB, como subsegmentos por meio de patches doAWSSDK. O X-Ray também pode se integrar automaticamente às funções do Lambda.

Se os componentes do aplicativo fizerem chamadas para serviços externos que não conseguem configurar e instalar o daemon do X-Ray ou instrumentar o código, você poderá criarsubsegmentos para agrupar chamadas para serviços externos. Correlaciona X-Ray CloudWatch logs e métricas com os rastreamentos de aplicativos se você estiver usando oSDK do AWS X-Ray for Java, o que significa que você pode analisar rapidamente as métricas e registros relacionados para solicitações.

Implantar o daemon X-Ray para rastrear aplicativos e serviços no Amazon EC2

É necessário instalar e executar o daemon do X-Ray nas instâncias do EC2 nas quais os componentes do aplicativo ou os microsserviços são executados. É possível usar umscript de dados do usuáriopara implantar o daemon X-Ray quando as instâncias do EC2 são provisionadas ou você pode incluí-lo no processo de compilação da AMI se você criar suas próprias AMIs. Isso pode ser particularmente útil quando as instâncias do EC2 são efêmeras.

Você deve usar o State Manager para garantir que o daemon X-Ray esteja instalado consistentemente em suas instâncias do EC2. Para o Amazon EC2Janelainstâncias, você pode usar o Systems ManagerAWSDocumento do RunPowerShellScriptPara executar oScript do Windowsque faz download e instala o agente do X-Ray. Para instâncias do EC2 no Linux, você pode usar oAWSDocumento -RunShellScript para executar o script Linux quefaz download e instala o agente como um serviço.

É possível usar o Systems ManagerAWSDocumento do RunRemoteScriptpara executar o script em um ambiente de várias contas. Você deve criar um bucket do S3 acessível a partir de todas as suas contas e recomendamosCriar um bucket do S3 com uma política de bucket baseada na organizaçãoSe você usar oAWS Organizations. Em seguida, você carrega os scripts para o bucket do S3, mas certifique-se de que a função do IAM para suas instâncias do EC2 tenha permissão para acessar o bucket e os scripts.

Você também pode configurar o State Manager para associar os scripts a instâncias do EC2 que têm o agente X-Ray instalado. Como todas as instâncias do EC2 podem não exigir ou usar o X-Ray, você pode direcionar a associação com tags de instância. Por exemplo, você pode criar a associação do State Manager com base na presença do`InstallAWSXRayDaemonWindows`ou`InstallAWSXRayDaemonLinux`tags.

Implantar o daemon X-Ray para rastrear aplicativos e serviços no Amazon ECS ou no Amazon EKS

Você pode implantar oDaemon X-Raycomo um contêiner sidecar para cargas de trabalho baseadas em contêiner, como Amazon ECS ou Amazon EKS. Seus contêineres de aplicativos podem se conectar ao contêiner sidecar com vinculação de contêiner se você usar o Amazon ECS ou se o contêiner pode se conectar diretamente ao contêiner sidecar no localhost se você usarModo de rede awsvpc.

Para o Amazon EKS, você pode definir o daemon X-Ray na definição de pod do aplicativo e, em seguida, seu aplicativo pode se conectar ao daemon via localhost na porta de contêiner especificada.

Configurando o Lambda para rastrear solicitações para o X-Ray

Seu aplicativo pode incluir chamadas para funções do Lambda. Não é necessário instalar o daemon do X-Ray para o Lambda porque o processo do daemon é totalmente gerenciado pelo Lambda e não pode ser configurado pelo usuário. Você pode ativá-lo para sua função do Lambda usando oAWS Management Consolee Verificar oRastreamento ativoopção no console X-Ray.

Para mais instrumentação, você pode empacotar o X-Ray SDK com sua função do Lambda para registrar chamadas de saída e adicionar anotações ou metadados.

Instrumentar suas aplicações para X-Ray

Você deve avaliar o SDK do X-Ray que se alinha à linguagem de programação do aplicativo e classificar todas as chamadas feitas pelo aplicativo para outros sistemas. Revise os clientes fornecidos pela biblioteca que você escolheu e veja se o SDK pode instrumentar automaticamente o rastreamento para a solicitação ou resposta do aplicativo. Determine se os clientes fornecidos pelo SDK podem ser usados para outros sistemas downstream. Para sistemas externos que o aplicativo chama e que você não pode instrumentar com o X-Ray, você deve criar subsegmentos personalizados para capturá-los e identificá-los em suas informações de rastreamento.

Ao instrumentar seu aplicativo, certifique-se de criar anotações para ajudá-lo a identificar e pesquisar solicitações. Por exemplo, seu aplicativo pode usar um identificador para clientes, como`customer id`, ou segmente usuários diferentes com base em sua função no aplicativo.

Você pode criar um máximo de 50 anotações para cada rastreamento, mas pode criar um objeto de metadados contendo um ou mais campos, desde que o documento de segmento não exceda 64 kilobytes. Você deve usar seletivamente anotações para localizar informações e usar o objeto de metadados para fornecer mais contexto que ajuda a solucionar problemas da solicitação depois que ela for localizada.

Configurar regras de amostragem do X-Ray

ByPersonalizar regras de amostragem, você pode controlar a quantidade de dados gravados e modificar o comportamento de amostragem sem modificar ou reimplantar seu código. As regras

de amostragem informam ao X-Ray SDK do número de solicitações a serem registradas para um conjunto de critérios. Por padrão, o X-Ray SDK registraa primeira solicitação a cada segundo e cinco por cento de quaisquer solicitações adicionais. Uma solicitação por segundo é o reservatório. Isso garante que pelo menos um rastreamento seja registrado a cada segundo à medida que o serviço atende às solicitações. Cinco por cento é a taxa na qual as solicitações adicionais são amostradas além do tamanho do reservatório.

Você deve revisar e atualizar a configuração padrão para determinar um valor apropriado para sua conta. Seus requisitos podem variar nos ambientes de desenvolvimento, teste, teste de desempenho e produção. Você pode ter aplicativos que exigem suas próprias regras de amostragem com base na quantidade de tráfego que eles recebem ou no nível de criticidade. Você deve começar com uma linha de base e reavaliar regularmente se a linha de base atende aos seus requisitos.

Painéis e visualizações com o CloudWatch

Os painéis ajudam você a se concentrar rapidamente em áreas de preocupação para aplicativos e cargas de trabalho. O CloudWatch fornece painéis automáticos e você também pode criar facilmente painéis que usam CloudWatch Métricas do . CloudWatch painéis fornecem mais insights do que visualizar métricas isoladamente porque ajudam você a correlacionar várias métricas e identificar tendências. Por exemplo, um painel que inclui pedidos recebidos, memória, utilização da CPU e conexões de banco de dados pode ajudá-lo a correlacionar alterações nas métricas de carga de trabalho em váriosAWSrecursos enquanto a contagem de pedidos está aumentando ou diminuindo.

Você deve criar painéis no nível da conta e do aplicativo para monitorar cargas de trabalho e aplicativos. Você pode começar usando CloudWatch painéis automáticos, que sãoAWSpainéis de nível de serviço pré-configurados com métricas específicas do serviço. Painéis de serviço automático exibem todo o padrão CloudWatch Métricas do serviço. Os painéis automáticos representam gráficos de todos os recursos usados para cada métrica de serviço e ajudam você a identificar rapidamente recursos outlier em sua conta. Isso pode ajudá-lo a identificar recursos com alta e baixa utilização, o que pode ajudá-lo a otimizar seus custos.

Criar painéis de serviços

Você pode criar painéis de serviços cruzados exibindo o painel automático de nível de serviço para umAWSserviço e usando oAdicionar ao painelopção doAçõesmenu. Em seguida, você pode adicionar métricas de outros painéis automáticos ao novo painel e remover métricas para restringir o foco do painel. Você também deve adicionar suas próprias métricas personalizadas para rastrear as principais observações (por exemplo, pedidos recebidos ou transações por segundo). Criar seu próprio painel personalizado entre serviços ajuda você a se concentrar nas métricas mais relevantes para sua carga de trabalho. Recomendamos que você crie painéis de controle entre serviços em nível de conta que cobrem as principais métricas e exibem todas as cargas de trabalho em uma conta.

Se você tiver um espaço de escritório central ou uma área comum para suas equipes de operações em nuvem, poderá exibir o CloudWatch painel em um monitor de TV grande em modo de tela cheia com atualização automática.

Criando painéis específicos de aplicativos ou cargas de trabalho

Recomendamos que você crie painéis específicos de aplicativos e cargas de trabalho que se concentrem nas principais métricas e recursos para cada aplicativo crítico ou carga de trabalho em seu ambiente de produção. Painéis específicos de aplicativos e cargas de trabalho se concentram em seu aplicativo personalizado ou métricas de carga de trabalho e importantesAWSmétricas de recursos que influenciam seu desempenho.

Você deve avaliar e personalizar regularmente seu CloudWatch painéis de aplicativos ou cargas de trabalho para rastrear as principais métricas após a ocorrência de incidentes. Você também deve atualizar painéis específicos do aplicativo ou da carga de trabalho quando os recursos forem introduzidos ou desativados. As atualizações de painéis específicos de carga de trabalho e aplicativos devem ser uma atividade necessária para a melhoria contínua da qualidade, além de registro e monitoramento.

Criar painéis entre contas ou entre regiões

AWSos recursos são principalmente regionais e as métricas, alarmes e painéis são específicos da Região em que os recursos são implantados. Isso pode exigir que você altere Regiões para exibir métricas, painéis e alarmes para cargas de trabalho e aplicativos entre regiões. Se você separar seus aplicativos e cargas de trabalho em várias contas, também será necessário autenticar novamente e fazer login em cada conta. No entanto, CloudWatch oferece suporte à visualização de dados entre contas e entre regiões a partir de uma única conta, o que significa que você pode visualizar métricas, alarmes, painéis e widgets de registro em uma única conta e Região. Isso é muito útil se você tiver uma conta centralizada de registro e monitoramento.

Os proprietários de contas e os proprietários da equipe de aplicativos devem criar painéis para aplicativos entre regiões específicos da conta para monitorar efetivamente as principais métricas em um local centralizado. Os painéis do CloudWatch suportam automaticamente widgets entre regiões, o que significa que você pode criar um painel que inclui métricas de várias regiões sem configuração adicional.

Uma exceção importante é a CloudWatch Widget Logs Insights porque os dados de log só podem ser exibidos para a conta e a região em que você está conectado no momento. Você pode criar métricas específicas da região a partir de seus logs usando filtros de métrica e essas métricas podem ser exibidas em um painel entre regiões. Em seguida, você pode alternar para a região específica quando precisar analisar ainda mais esses logs.

As equipes de operações devem criar um painel centralizado que monitore importantes métricas entre contas e entre regiões. Por exemplo, você pode criar um painel de controle entre contas que inclua a utilização agregada da CPU em cada conta e região. Você também pode usarMatemática métricaPara agregar e painel de dados em várias contas e regiões.

Usando matemática métrica para ajustar a observabilidade e o alarmante

Você pode usar matemática métrica para ajudar a calcular métricas em formatos e expressões relevantes para suas cargas de trabalho. As métricas calculadas podem ser salvas e visualizadas em um painel para fins de rastreamento. Por exemplo, as métricas de volume padrão do Amazon EBS fornecem o número de leitura (`VolumeReadOps`) e escreva (`VolumeWriteOps`) operações realizadas durante um período específico.

No entanto,AWSfornece diretrizes sobre o desempenho do volume do Amazon EBS em IOPS. Você pode representar gráficos e calcular as IOPS para o volume do Amazon EBS em matemática métrica adicionando o`VolumeReadOpse``VolumeWriteOpse` depois dividindo pelo período escolhido para essas métricas.

Neste exemplo, resumimos as IOPS no período e depois dividimos pela duração do período para obter o IOPS. Em seguida, você pode definir um alarme contra essa expressão matemática métrica para alertá-lo quando o IOPS do volume se aproxima da capacidade máxima para seu tipo de volume. Para obter mais informações e exemplos sobre o uso de matemática métricas para monitorar sistemas de arquivos Amazon Elastic File System (Amazon EFS) com CloudWatch métricas, consulteAmazônia CloudWatch a matemática métrica simplifica o monitoramento quase em tempo real de seus sistemas de arquivos do Amazon EFS e muito maisnoAWSBlog.

Usando painéis automáticos para Amazon ECS, Amazon EKS e Lambda com CloudWatchContainer Insights e CloudWatch Lambda Insights

O CloudWatch Container Insights cria painéis dinâmicos e automáticos para cargas de trabalho de contêiner em execução no Amazon ECS e no Amazon EKS. Você deve habilitar o Container Insights para ter observabilidade de informações de CPU, memória, disco, rede e diagnóstico, como falhas de reinicialização do contêiner. O Container Insights gera painéis dinâmicos que você

pode filtrar rapidamente nos níveis de cluster, instância ou nó de contêiner, serviço, tarefa, pod e contêiner individual. Container Insightsestá configurado no nível de instância de cluster e nó ou contêinerDependendo doAWSserviço.

Similar a Container Insights, CloudWatch O Lambda Insights cria painéis dinâmicos e automáticos para suas funções do Lambda. Essa solução coleta, agrega e resume métricas no nível do sistema, incluindo tempo da CPU, memória, disco e rede. Ele também coleta, agrega e resume informações de diagnóstico, como inicializações a frio e desligamentos do operador do Lambda para ajudar a isolar e resolver rapidamente problemas com as funções do Lambda. O Lambda está habilitado no nível da função e não requer nenhum agente.

O Container Insights e o Lambda Insights também ajudam você a mudar rapidamente para o aplicativo ou logs de desempenho, rastreamentos de X-Ray e um mapa de serviço para visualizar suas cargas de trabalho de contêiner. Ambos usam o CloudWatch Formato de métricas incorporadas para capturar CloudWatch Métricas e logs de desempenho.

Você pode criar um compartilhado CloudWatch painel para sua carga de trabalho que usa as métricas capturadas pelo Container Insights e pelo Lambda Insights. Você pode fazer isso filtrando e visualizando o painel automático do CloudWatch Container Insights e depois escolher oAdicionar ao painelopção que permite adicionar as métricas exibidas a um painel padrão do CloudWatch. Em seguida, você pode remover ou personalizar as métricas e adicionar outras métricas para representar corretamente sua carga de trabalho.

Integração do CloudWatch com oAWSserviços

AWSfornece muitos serviços que incluem opções de configuração adicionais para registro em log e métricas. Esses serviços geralmente permitem que você configure CloudWatch Registros para saída de log e CloudWatch métricas para saída de métricas. A infraestrutura subjacente usada para fornecer esses serviços é gerenciada porAWSeÉ inacessível, mas você pode usar as opções de registro e métrica para seus serviços provisionados para obter mais insights e solucionar problemas. Por exemplo, você pode publicarVPC Flow Logs no CloudWatch Watch, ou você também podeConfigurar instâncias do Amazon Relational Database Service (Amazon RDS) para publicar logs no CloudWatch.

MostAWSOs serviços registram suas chamadas de API com oIntegração do comAWS CloudTrail. CloudTrail tambémO oferece suporte à integração com o CloudWatch Logse isso significa que você pode pesquisar e analisar a atividade emAWSServiços da . Você também pode usar a Amazon CloudWatch Eventos ou Amazon EventBridge para criar e configurar automação e notificações com CloudWatch Regras de eventos de eventos para ações específicas realizadas emAWSServiços da . Certos serviçosIntegração do diretamentecom CloudWatch Eventos e EventBridge. Você também podecriar eventos entregues por meio do CloudTrail.

Amazon Managed Grafana para painéis e visualização

Amazon Managed Grafanapode ser usado para observar e visualizar seuAWScargas de trabalho. O Amazon Managed Grafana ajuda você a visualizar e analisar seus dados operacionais em grande escala. ao Grafanaé uma plataforma de análise de código aberto que ajuda você a consultar, visualizar, alertar e entender suas métricas onde quer que elas estejam armazenadas. O Amazon Managed Grafana é particularmente útil se sua organização já usa o Grafana para visualização de cargas de trabalho existentes e você deseja estender a cobertura paraAWScargas de trabalho. Você pode usar o Amazon Managed Grafana com CloudWatch deadicionando-o como uma fonte de dados, o que significa que você pode criar visualizações usando CloudWatchMétricas do . O Amazon Managed Grafana oferece suporteAWS Organizationse você pode centralizar painéis usando CloudWatch métricas de várias contas e regiões.

A tabela a seguir fornece as vantagens e considerações para usar o Amazon Managed Grafana em vez de CloudWatch para painel do. Uma abordagem híbrida pode ser adequada com base nos diferentes requisitos de seus usuários finais, cargas de trabalho e aplicativos.

Crie visualizações e painéis que se integram a fontes de dados compatíveis com o Amazon Managed Grafana e o Grafana de código aberto	O Amazon Managed Grafana ajuda você a criar visualizações e painéis de várias fontes de dados diferentes, incluindo CloudWatch Métricas do . O Amazon Managed Grafana inclui várias fontes de dados integradas que abrangemAWSserviços, software de código aberto e software COTS. Para obter mais informações sobre isso, consulteFontes de dados integradasna documentação do Amazon Managed Grafana. Você também pode adicionar suporte para mais fontes de dados atualizando seu espaço de trabalho paraEmpresa ao Grafana. O Grafana também suportaplug-ins de fonte de dadosque permitem que você se comunique com diferentes sistemas externos. CloudWatchOs painéis do exigem um CloudWatch Métrica do ou CloudWatch Consulta do Logs Insights

	para que os dados sejam exibidos em um CloudWatch Painel do.
Gerencie o acesso à sua solução de painel separadamente doAWSacesso da conta da	O Amazon Managed Grafana exige o uso deAWS IAM Identity Center(Centro de identidade do IAM) eAWS Organizationspara autenticação e autorização. Isso permite que você autentique usuários no Grafana usando a federação de identidades que você já pode usar com o IAM Identity Center ouAWS Organizations. No entanto, se você não estiver usando o IAM Identity Center ouAWS Organizations, em seguida, ele é configurado como parte do processo de configuração do Amazon Managed Grafana. Isso pode se tornar um problema se sua organização tiver limitado o uso do IAM Identity Center ouAWS Organizations.
Ingerir e acessar dados em várias contas e regiões comAWS Organizationsintegração	O Amazon Managed Grafana se integra ao AmazonAWS Organizationspara permitir que você leia dados deAWSfontes como CloudWatch e o Amazon OpenSearch Serviço em todas as suas contas. Isso possibilita a criação de painéis que exibem visualizações usando dados em suas contas. Para habilitar automaticamente o acesso aos dados emAWS Organizations, você precisa configurar o Amazon Managed Grafana noAWS Organizationsconta de gerenciamento Isso não é recomendado com base emAWS OrganizationsPráticas recomendadas para a conta de gerenciamento. Em contraste, CloudWatch também O oferece suporte a painéis entre contas e entre regiões para o CloudWatch métricas.

Use widgets de visualização avançada e definições do Grafana disponíveis na comunidade de código aberto	O Grafana fornece uma grande coleção de visualizações que você pode usar ao criar seus painéis. Há também uma grande biblioteca de painéis contribuídos pela comunidade que você pode editar e reutilizar de acordo com suas necessidades.
Use painéis com implantações novas e existentes do Grafana	Se você já usa o Grafana, pode importar e exportar painéis de suas implantações do Grafana e personalizá-los para uso no Amazon Managed Grafana. O Amazon Managed Grafana permite que você padronize o Grafana como sua solução de painel.
Configuração e configuração avançadas para espaços de trabalho, permissões e fontes de dados	O Amazon Managed Grafana permite que você crie vários espaços de trabalho do Grafana que têm seu próprio conjunto de fontes de dados, usuários e políticas configuradas. Isso pode ajudá-lo a atender a requisitos de casos de uso mais avançados, bem como configura ções avançadas de segurança. Os recursos avançados podem exigir que suas equipes aumentem sua experiência com o Grafana se ainda não tiverem essas habilidades.

Projetando e implementando registros e monitoramento com CloudWatch PERGUNTAS FREQUENTES

Esta seção fornece respostas para perguntas geralmente levantadas sobre como projetar e implementar a solução de registro e monitoramento com o CloudWatch.

Onde eu armazeno meu CloudWatch Arquivos de configuração?

O CloudWatch agent for Amazon EC2 pode aplicar vários arquivos de configuração armazenados no CloudWatch Diretório de configuração. Idealmente, você deve armazenar sua configuração do CloudWatch como um conjunto de arquivos, pois você pode controlar a versão e usá-los novamente em várias contas e ambientes. Para obter mais informações sobre isso, consulte oGerenciando CloudWatch configuraçõesSeção deste guia. Como alternativa, você pode armazenar seus arquivos de configuração em um repositório no GitHub e automatize a recuperação dos arquivos de configuração quando uma nova instância do EC2 é provisionada.

Como posso criar um ticket na minha solução de gerenciamento de serviços quando um alarme é gerado?

Você integra seu sistema de gerenciamento de serviços a um tópico do Amazon Simple Notification Service (Amazon SNS) e configura o CloudWatch alarme para notificar o tópico do SNS quando um alarme é acionado. Seu sistema integrado recebe a mensagem do SNS e pode criar um ticket usando as APIs ou SDKs dos sistemas de gerenciamento de serviços.

Como posso usar CloudWatch para capturar arquivos de log em meus contêineres?

As tarefas do Amazon ECS e os pods do Amazon EKS podem ser configurados para enviar automaticamente a saída STDOUT e STDERR para o CloudWatch. A abordagem recomendada para registrar aplicativos em contêineres é fazer com que os contêineres enviem sua saída para STDOUT e STDERR. Isso também é abordado noManifesto do aplicativo de doze fatores.

No entanto, se você quiser enviar arquivos de log específicos para CloudWatch em seguida, você pode montar um volume no pod do Amazon EKS ou na definição de tarefas do Amazon ECS para

onde seu aplicativo gravará seus arquivos de lote e usará um contêiner sidecar para Fluentd ou Fluent Bit para enviar os logs para o CloudWatch. Você deve considerar a vinculação simbólica de um arquivo de log específico em seu contêiner para `/dev/stdout` e `/dev/stderr`. Para obter mais informações sobre isso, consulte Exibir registros de um contêiner ou serviço na documentação do Docker.

Como faço para monitorar problemas de saúde para AWS serviços?

Você pode usar o AWS Health Dashboard monitorar AWS Eventos de integridade da saúde. Você também pode consultar o aws-health-tools GitHub repositório para soluções de automação de amostra relacionadas a AWS Eventos de integridade da saúde.

Como posso criar um personalizado CloudWatch métrica quando não existe suporte de agente?

É possível usar o formato de métrica incorporado para ingerir métricas no CloudWatch. Você também pode usar AWS SDK (por exemplo, put_metric_data), AWS CLI (por exemplo, put-metric-data), ou AWS API (por exemplo, PutMetricData) para criar métricas personalizadas do Você deve considerar como qualquer lógica personalizada será mantida a longo prazo. Uma abordagem seria usar o Lambda com suporte integrado ao formato métrico incorporado para criar suas métricas, juntamente com um CloudWatch Eventos do evento regra de agendamento para estabelecer o período para a métrica.

Como faço para integrar minhas ferramentas de monitoramento e registro existentes com AWS?

Você deve consultar as orientações fornecidas pelo fornecedor de software ou serviço para integração com AWS. Talvez você consiga usar o software do agente, o SDK ou uma API fornecida para enviar registros e métricas para a solução deles. Você também pode usar uma solução de código aberto, como Fluentd ou Fluent Bit, configurada de acordo com as especificações do fornecedor. Você também pode usar o AWS SDK e CloudWatch Registra filtros de assinatura com o Lambda e Kinesis Data Streams para criar processadores de log e remetentes personalizados. Finalmente, você também deve considerar como integrará o software se estiver usando várias contas e regiões.

Recursos

Introdução

- AWSWell-Architected

Resultados de negócios direcionados

- logging-monitoring-apg-guide-exemplos
- Seis vantagens da computação em nuvem

Planejando sua CloudWatch implantação

- Terminologia e conceitos do AWS Organizations
- AWS Systems ManagerConfiguração rápida
- Coletar métricas e logs de instâncias do Amazon EC2 e servidores on-premises com o CloudWatch atendente
- cloudwatch-config-s3-bucket.yaml
- Criar o arquivo de configuração do CloudWatch atendente com o assistente
- Enterprise DevOps: Por que você deve executar o que você constrói
- Exportar dados de log para o Amazon S3
- Controle de acesso refinado no Amazon OpenSearch Service
- Cotas do Lambda
- Criar ou editar manualmente o arquivo de configuração do CloudWatch atendente
- Processamento em tempo real de dados de log com assinaturas
- Ferramentas para desenvolverAWS

Configurar o CloudWatch atendente para instâncias do EC2 e servidores on-premises

- Dimensões de métrica do Amazon EC2

- Instâncias com capacidade de intermitência
- CloudWatch conjuntos de métricas predefinidas do atendente
- Coletar métricas de processo com o plugin procstat
- Configurando o CloudWatch agente para o procstat
- Habilitar ou desabilitar o monitoramento detalhado para instâncias
- Ingerir logs de alta cardinalidade e gerar métricas com formato de métricas CloudWatch incorporadas
- Trabalhar com grupos e fluxos de log
- Listar as CloudWatch métricas disponíveis para as instâncias
- PutLogEvents
- Recuperar métricas personalizadas com o collectd
- Recuperar métricas personalizadas com o StatsD

CloudWatch abordagens de instalação de agentes para Amazon EC2 e servidores locais

- Crie uma função de serviço do IAM para um ambiente híbrido
- Criar uma ativação de instância gerenciada para um ambiente híbrido
- Criar funções e usuários do IAM para uso com o CloudWatch atendente
- Baixar e configurar o CloudWatch atendente usando a linha de comando
- Como posso configurar servidores locais que usam o agente Systems Manager e o CloudWatch agente unificado para usar somente credenciais temporárias?
- Pré-requisitos para operações de conjunto de pilhas
- Usando instâncias spot

Registro em log e monitoramento no Amazon ECS

- amazon-cloudwatch-logs-for-bit fluente
- CloudWatch Métricas do Amazon ECS
- Métricas do Amazon ECS Container Insights

- Agente do contêiner do Amazon ECS
- Tipos de inicialização do Amazon ECS
- Implantar o CloudWatch atendente para coletar métricas no nível de instância do EC2 no Amazon ECS
- ecs_cluster_with_cloudwatch_linux.yaml
- ecs_cw_emf_example
- ecs_firelense_emf_example
- ecs-task-nginx-firelense.json
- Recuperando metadados de AMI otimizados para o Amazon ECS
- Usar o driver de log awslogs
- Usar as bibliotecas clientes para gerar logs de formato de métricas incorporadas

Registro em log e monitoramento no Amazon EKS

- Registro em log do ambiente de gerenciamento do Amazon EKS
- amazon_eks_managed_node_group_launch_config.yaml
- Nós do Amazon EKS
- amazon-eks-nodegroup.yaml
- Contrato de nível de serviço do Amazon EKS
- Monitoramento de métricas do Container Insights Prometheus
- Controle as métricas do plano com o Prometheus
- Implantar o painel do Kubernetes (interface do usuário da Web)
- Registro de Fargate
- Fluent Bit para Amazon EKS no Fargate
- Como capturar registros de aplicativos ao usar o Amazon EKS no Fargate
- Instalar o CloudWatch atendente para coletar métricas do Prometheus
- Instalar o servidor de métricas do Kubernetes
- kubernetes/painel
- Autoescalador de pod horizontal Kubernetes
- Componentes do plano de controle Kubernetes

- Pods do Kubernetes
- Suporte do modelo de execução
- Grupos de nós gerenciados
- Comportamento de atualização do nó gerenciado
- servidor de métricas
- Monitoramento do Amazon EKS no Fargate usando Prometheus e Grafana
- prometheus_jmx
- prometheus/jmx_exporter
- Extrair outras fontes do Prometheus e importar essas métricas
- Nós autogerenciados
- Enviar registros para CloudWatch registros
- Configurar o FluentD como um DaemonSet para enviar logs para CloudWatch os logs
- Configurar amostra de workload do Java/JMX no Amazon EKS e no Kubernetes
- Tutorial para adicionar um novo destino de extração do Prometheus: métricas do servidor de API do Prometheus
- Escalador automático Vertical Pod

Registro e métricas paraAWS Lambda

- Erros de invocação do Lambda
- logging — Facilidade de registro para Python
- Usar as bibliotecas clientes para gerar logs de formato de métricas incorporadas
- Trabalhar com métricas de funções Lambda

Pesquisando e analisando registros CloudWatch

- A família Beats
- Elastic Logstash
- Pilha elástica
- Streaming CloudWatch registra dados para o Amazon OpenSearch Service

Opções alarmantes com CloudWatch

- amazon-cloudwatch-auto-alarms
- AWSConector de gerenciamento de serviços para o Jira Service Management
- AWSConector de gerenciamento de serviços para ServiceNow

Monitorando a disponibilidade de aplicativos e serviços

- Configurar failover de DNS

Rastreando aplicativos comAWS X-Ray

- Rede de tarefas do Amazon ECS
- Configurar regras de amostragem no console do X-Ray
- Execute PowerShell comandos ou scripts do Windows
- Executar o daemon do X-Ray no Amazon EC2
- Enviar dados de rastreamento para o X-Ray
- Gráfico de serviços no X-Ray

Painéis e visualizações com CloudWatch

- O Amazon CloudWatch Metric Math simplifica o monitoramento quase em tempo real de seus sistemas de arquivos Amazon EFS
- Configurando o CloudWatch Container Insights
- Usar matemática métricas

CloudWatch integração comAWS serviços

- Serviços e integrações compatíveis com o AWS CloudTrail
- CloudWatch Eventos, exemplos de eventos de serviços suportados
- Eventos entregues via CloudTrail
- Monitorando arquivos de CloudTrail log com CloudWatch Logs

- Publicar logs de mecanismos de banco de dados no CloudWatch Logs
- Publicar logs de fluxo no CloudWatch Logs

Amazon Managed Grafana para painel e visualização

- Práticas recomendadas para a conta de gerenciamento noAWS Organizations
- Fontes de dados integradas para o Amazon Managed Grafana
- Painéis entre contas e regiões em CloudWatch
- Plugins Grafana

Histórico do documento

A tabela a seguir descreve alterações significativas neste guia. Se você quiser ser notificado sobre future atualizações, você pode assinar um feed RSS.

Alteração	Descrição	Data
Informações de registro atualizadas	Atualizou a seção sobre registro paraAWS Lambda.	17 de abril de 2023
Informações de configuração atualizadas	Atualizou e renomeou a seção sobre criação e armazenamento de CloudWatch configurações.	9 de fevereiro de 2023
Informações de métricas atualizadas	Atualizou as informações de métricas personalizadas do aplicativo na seção Métricas do Amazon ECS.	31 de janeiro de 2023
Avisos de pré-visualização removidos	O Amazon Managed Grafana está disponível para o público.	25 de maio de 2022
Seção removida	CloudWatch O SDK Metrics não é mais compatível.	7 de janeiro de 2022
Publicação inicial	—	30 de abril de 2021

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

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

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

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

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade (ACID)

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

controle de acesso por atributo (ABAC)

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

fonte de dados autorizada

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

Availability Zone (zona de disponibilidade)

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

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

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

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

B

bot ruim

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

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

acesso em vidro quebrado

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços conteinerizados na AWS.

planejamento de continuidade de negócios (BCP)

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

C

CAF

Consulte Estrutura de adoção da AWS nuvem.

implantação canária

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

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja a integração e a entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de Excelência da Nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as postagens do CCoE no blog AWS Cloud Enterprise Strategy.

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam quando migram para a AWS nuvem:

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

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

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

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

desvio de dados

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

dados em trânsito

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

malha de dados

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta

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

implantação

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

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

recuperação de desastres (DR)

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

DML

Consulte linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja a recuperação de desastres.

detecção de deriva

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

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

computação de borda

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

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o endpoint do serviço.

serviço de endpoint

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

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

environment (ambiente)

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

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

epic

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

ERP

Consulte planejamento de recursos corporativos.

análise exploratória de dados (EDA)

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

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

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a filial.

recursos

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

importância do recurso

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

transformação de recursos

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

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

FGAC

Veja o controle de acesso refinado.

controle de acesso refinado (FGAC)

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

migração flash-cut

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

G

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

estratégia greenfield

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

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

barreira de proteção

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

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

I

IaC

Veja a infraestrutura como código.

Política baseada em identidade

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

aplicação ociosa

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

IIoT

Veja a Internet das Coisas industrial.

infraestrutura imutável

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

VPC de entrada (admissão)

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

migração incremental

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

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

O processo de provisionamento e gerenciamento da infraestrutura de uma aplicação por meio de um conjunto de arquivos de configuração. A IaC foi projetada para ajudar você a centralizar

o gerenciamento da infraestrutura, padronizar recursos e escalar rapidamente para que novos ambientes sejam reproduzíveis, confiáveis e consistentes.

Internet das Coisas Industrial (IIoT)

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

VPC de inspeção

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

Internet das Coisas (IoT)

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

interpretabilidade

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

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em etiquetas.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

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

ambientes inferiores

Veja o ambiente.

M

machine learning (ML)

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

ramificação principal

Veja a filial.

malware

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

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

conta-membro

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

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens (MQTT)

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

microsserviço

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

arquitetura de microsserviços

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

Programa de Aceleração da Migração (MAP)

Um AWS programa que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a

compensar o custo inicial das migrações. O MAP inclui uma metodologia de migração para executar migrações legadas de forma metódica e um conjunto de ferramentas para automatizar e acelerar cenários comuns de migração.

migração em escala

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

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações, analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte discussão sobre fábricas de migração e o guia do Cloud Migration Factory neste conjunto de conteúdo.

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja o aprendizado de máquina.

modernização

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

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte Avaliar a preparação para modernização de aplicações na AWS Cloud.

aplicações monolíticas (monólitos)

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

MAPA

Consulte Avaliação do portfólio de migração.

MQTT

Consulte Transporte de telemetria de enfileiramento de mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja o controle de acesso de origem.

CARVALHO

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

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

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

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

OPC-UA

Consulte Comunicação de processo aberto — Arquitetura unificada.

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

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (OT)

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

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

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

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

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

OU

Veja a análise de prontidão operacional.

NÃO

Veja a tecnologia operacional.

VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A Arquitetura de referência de segurança da AWS

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

P

limite de permissões

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

informações de identificação pessoal (PII)

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

PII

Veja as informações de identificação pessoal.

manual

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

PLC

Consulte controlador lógico programável.

AMEIXA

Veja o gerenciamento do ciclo de vida do produto.

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pressão de predicados

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

controle preventivo

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

principal (entidade principal)

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

Privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja o ambiente.

controlador lógico programável (PLC)

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

pseudonimização

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

publicar/assinar (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

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

ransomware

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

Matriz RASCI

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

RCAC

Veja o controle de acesso por linha e coluna.

réplica de leitura

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

rearquiteta

Veja 7 Rs.

objetivo de ponto de recuperação (RPO)

Período de tempo aceitável máximo desde o último ponto de recuperação de dados. Determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

Região

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

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

rotação

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

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

S

SAML 2.0

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

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

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

controle de segurança

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

fortalecimento da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

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

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes

de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte Abordagem em fases para modernizar aplicativos no. Nuvem AWS

CUSPE

Veja um único ponto de falha.

esquema de estrelas

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

padrão strangler fig

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

sub-rede

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

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

Uma abordagem na qual os desenvolvedores criam e testam recursos localmente em uma ramificação de recursos e, em seguida, mesclam essas alterações na ramificação principal. A

ramificação principal é então criada para os ambientes de desenvolvimento, pré-produção e produção, sequencialmente.

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o ambiente.

V

aspiração

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

controle de versões

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

emparelhamento de VPC

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

vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte o AWS Workload Qualification Framework.

escreva uma vez, leia muitas (WORM)

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

Z

exploração de dia zero

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

vulnerabilidade de dia zero

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

aplicação zumbi

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

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