Conception et mise en œuvre de la journalisation et de la surveillance avec Amazon CloudWatch

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Conception et mise en œuvre de la journalisation et de la surveillance avec Amazon CloudWatch

Table of Contents

Conception et mise en œuvre de la journalisation et de la surveillance avec Amazon CloudWatch

Khurram Nizami, Amazon Web Services ()AWS

Avril 2023 (historique du document)

Ce guide vous aide à concevoir et à implémenter la journalisation et la surveillance avec Amazon CloudWatch et les services de gestion et de gouvernance associés à Amazon Web Services (AWS) pour les charges de travail qui utilisent des instances Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) et des serveurs sur site. AWS Lambda Le guide est destiné aux équipes opérationnelles, aux DevOps ingénieurs et aux ingénieurs d'applications qui gèrent les charges de travail sur le AWS cloud.

Votre approche de journalisation et de surveillance doit être basée sur les six piliers du AWS Well-Architected Framework. Ces piliers sont l'excellence opérationnelle, la sécurité, la fiabilité, l'efficacité des performances et l'optimisation des coûts. Une solution de surveillance et d'alarme bien conçue améliore la fiabilité et les performances en vous aidant à analyser et à ajuster votre infrastructure de manière proactive.

Ce guide ne traite pas en détail de la journalisation et de la surveillance à des fins de sécurité ou d'optimisation des coûts, car ces sujets nécessitent une évaluation approfondie. De nombreux AWS services prennent en charge la journalisation et la surveillance de la sécurité AWS CloudTrailAWS Config, notamment Amazon Inspector, Amazon Detective, Amazon Macie GuardDuty, Amazon et. AWS Security Hub CSPM Vous pouvez également utiliser AWS Cost ExplorerAWS Budgets, et les métriques CloudWatch de facturation pour optimiser les coûts.

Le tableau suivant décrit les six domaines auxquels votre solution de journalisation et de surveillance doit répondre.

Capture et ingestion de fichiers journaux et de métriques	Identifiez, configurez et envoyez les journaux et métriques du système et des applications aux AWS services provenant de différentes sources.

Recherche et analyse des journaux	Recherchez et analysez les journaux pour la gestion des opérations, l'identification des problèmes, le dépannage et l'analyse des applications.
Métriques de surveillance et alarmes	Identifiez les observations et les tendances de vos charges de travail et agissez en conséquence.
Surveillance de la disponibilité des applications et des services	Réduisez les temps d'arrêt et améliorez votre capacité à atteindre les objectifs de niveau de service en surveillant en permanence la disponibilité des services.
Applications de traçage	Suivez les demandes d'applications dans les systèmes et les dépendances externes pour affiner les performances, effectuer une analyse des causes premières et résoudre les problèmes.
Création de tableaux de bord et de visualisations	Créez des tableaux de bord qui mettent l'accent sur les mesures et les observations pertinentes pour vos systèmes et vos charges de travail, ce qui contribue à l'amélioration continue et à la découverte proactive des problèmes.

CloudWatch peut répondre à la plupart des exigences de journalisation et de surveillance et fournit une solution fiable, évolutive et flexible. De nombreux AWS services fournissent automatiquement des CloudWatch métriques, en plus de l'intégration de la CloudWatch journalisation à des fins de surveillance et d'analyse. CloudWatch fournit également des agents et des pilotes de journal pour prendre en charge diverses options de calcul telles que les serveurs (dans le cloud et sur site), les conteneurs et l'informatique sans serveur. Ce guide couvre également les AWS services suivants utilisés pour la journalisation et la surveillance :

- AWS Systems Manager Distributor, Systems Manager State Manager et Systems Manager Automation pour automatiser, configurer et mettre à jour l' CloudWatch agent pour vos EC2 instances et vos serveurs sur site

- Amazon OpenSearch Service pour l'agrégation, la recherche et l'analyse avancées des journaux
- Contrôles de santé et CloudWatchSynthetics d'Amazon Route 53 pour surveiller la disponibilité des applications et des services
- Amazon Managed Service pour Prometheus pour la surveillance des applications conteneurisées à grande échelle
- AWS X-Raypour le suivi des applications et l'analyse du temps d'exécution
- Amazon a géré Grafana pour visualiser et analyser des données provenant de sources multiples (par exemple, CloudWatch Amazon OpenSearch Service et Amazon Timestream)

Les services AWS informatiques que vous choisissez ont également une incidence sur la mise en œuvre et la configuration de votre solution de journalisation et de surveillance. Par exemple, CloudWatch sa mise en œuvre et sa configuration sont différentes pour Amazon EC2, Amazon ECS, Amazon EKS et Lambda.

Les responsables des applications et des charges de travail peuvent souvent oublier la journalisation et la surveillance ou les configurer et les implémenter de manière incohérente. Cela signifie que les charges de travail entrent en production avec une observabilité limitée, ce qui retarde l'identification des problèmes et augmente le temps nécessaire pour les dépanner et les résoudre. Votre solution de journalisation et de surveillance doit au minimum traiter la couche système pour les journaux et les métriques au niveau du système d'exploitation (OS), en plus de la couche application pour les journaux et les métriques des applications. Le guide propose une approche recommandée pour traiter ces deux couches dans différents types de calcul, y compris les trois types de calcul décrits dans le tableau suivant.

Instances immuables EC2 et de longue durée	Journaux et indicateurs du système et des applications sur plusieurs systèmes d'exploit ation (OSs) dans plusieurs AWS régions ou comptes.
Conteneurs	Journaux et métriques du système et des applications pour vos clusters Amazon ECS et Amazon EKS, y compris des exemples de différentes configurations.

Serverless (Sans serveur)	Journaux et métriques du système et des applications pour vos fonctions Lambda et considérations relatives à la personnalisation.

Ce guide fournit une solution de journalisation et de surveillance qui traite CloudWatch AWS des services associés dans les domaines suivants :

- Planification de votre CloudWatch déploiement— Considérations relatives à la planification de votre CloudWatch déploiement et conseils sur la centralisation de votre CloudWatch configuration.
- Configuration de l' CloudWatch agent pour les EC2 instances et les serveurs locaux— détails CloudWatch de configuration pour la journalisation et les métriques au niveau du système et de l'application.
- CloudWatch approches d'installation d'agents pour Amazon EC2 et les serveurs sur site— Approches d'installation de l' CloudWatch agent, y compris le déploiement automatique à l'aide de Systems Manager sur plusieurs régions et comptes.
- Journalisation et surveillance sur Amazon ECS — Conseils pour la configuration de la CloudWatch journalisation et des métriques au niveau du cluster et de l'application dans Amazon ECS.
- Journalisation et surveillance dans Amazon EKS — Conseils pour la configuration de la CloudWatch journalisation et des métriques au niveau du cluster et de l'application dans Amazon EKS.
- Surveillance de Prometheus sur Amazon EKS— Présente et compare Amazon Managed Service pour Prometheus CloudWatch avec la surveillance de Container Insights pour Prometheus.
- Journalisation et statistiques pour AWS Lambda— Conseils pour la configuration de CloudWatch vos fonctions Lambda.
- Recherche et analyse des connexions CloudWatch— Méthodes pour analyser vos journaux à l'aide d'Amazon CloudWatch Application Insights, CloudWatch Logs Insights et étendre l'analyse des journaux à Amazon OpenSearch Service.
- Des options alarmantes avec CloudWatch— Présente les CloudWatch alarmes et la détection des CloudWatch anomalies et fournit des conseils sur la création et la configuration des alarmes.
- Surveillance de la disponibilité des applications et des services— Présente et compare les CloudWatch tests de santé de Synthetics et de Route 53 pour une surveillance automatique de la disponibilité.

- Applications de suivi avec AWS X-Ray— Présentation et configuration du suivi des applications à l'aide de X-Ray pour Amazon EC2, Amazon ECS, Amazon EKS et Lambda
- Tableaux de bord et visualisations avec CloudWatch— Présentation des CloudWatch tableaux de bord pour une meilleure observabilité des charges de travail. AWS
- CloudWatch intégration avec les AWS services— Explique comment CloudWatch s'intègre aux différents AWS services.
- Amazon Managed Grafana pour les tableaux de bord et la visualisation— Présente et compare Amazon Managed Grafana à des CloudWatch fins de tableau de bord et de visualisation.

Des exemples de mise en œuvre sont utilisés dans ce guide dans ces domaines et sont également disponibles dans le GitHub référentiel AWS Samples.

Résultats commerciaux ciblés

La création d'une solution de journalisation et de surveillance conçue pour le AWS cloud est essentielle pour tirer parti des six avantages du cloud computing. Votre solution de journalisation et de surveillance doit aider votre service informatique à obtenir des résultats commerciaux bénéfiques pour vos processus commerciaux, vos partenaires commerciaux, vos employés et vos clients. Vous pouvez vous attendre aux quatre résultats suivants après avoir mis en œuvre une solution de journalisation et de surveillance alignée sur le AWS Well-Architected Framework :

Accélérez la préparation opérationnelle

L'activation d'une solution de journalisation et de surveillance est un élément important de la préparation d'une charge de travail pour le support et l'utilisation de la production. La préparation opérationnelle peut rapidement devenir un obstacle si vous vous fiez trop à des processus manuels, ce qui peut également réduire le délai de rentabilisation (TTV) de vos investissements informatiques. Une approche inefficace se traduit également par une observabilité limitée de vos charges de travail. Cela peut augmenter le risque de pannes prolongées, d'insatisfaction des clients et d'échec des processus commerciaux.

Vous pouvez utiliser les approches de ce guide pour standardiser et automatiser votre journalisation et votre surveillance AWS dans le cloud. Les nouvelles charges de travail nécessitent alors un minimum de préparation manuelle et d'intervention pour l'enregistrement et le suivi de la production. Cela permet également de réduire le temps et les étapes nécessaires pour créer des normes de journalisation et de surveillance à grande échelle pour différentes charges de travail sur plusieurs comptes et régions.

Améliorez l'excellence opérationnelle

Ce guide fournit plusieurs bonnes pratiques en matière de journalisation et de surveillance qui aident les diverses charges de travail à atteindre les objectifs commerciaux et à atteindre l'excellence opérationnelle. Ce guide fournit également des exemples détaillés et des modèles open source réutilisables que vous pouvez utiliser avec une approche d'infrastructure en tant que code (IaC) pour mettre en œuvre une solution de journalisation et de surveillance bien conçue à l'aide de services. AWS L'amélioration de l'excellence opérationnelle est itérative et nécessite une amélioration continue. Le guide fournit des suggestions sur la manière d'améliorer en permanence les pratiques d'exploitation forestière et de surveillance.

Améliorez la visibilité opérationnelle

Vos processus commerciaux et vos applications peuvent être pris en charge par différentes ressources informatiques et hébergés sur différents types de calcul, sur site ou dans le AWS cloud. Votre visibilité opérationnelle peut être limitée par des mises en œuvre incohérentes et incomplètes de votre stratégie de journalisation et de surveillance. L'adoption d'une approche complète de journalisation et de surveillance vous permet d'identifier, de diagnostiquer et de résoudre rapidement les problèmes liés à vos charges de travail. Ce guide vous aide à concevoir et à mettre en œuvre des approches visant à améliorer votre visibilité opérationnelle complète et à réduire le délai moyen de résolution (MTTR) des défaillances. Une approche complète de journalisation et de surveillance aide également votre entreprise à améliorer la qualité de service, à améliorer l'expérience des utilisateurs finaux et à respecter les accords de niveau de service (). SLAs

Élargissez les opérations et réduisez les frais généraux

Vous pouvez adapter les pratiques de journalisation et de surveillance à partir de ce guide pour prendre en charge plusieurs régions et comptes, des ressources éphémères et plusieurs environnements. Le guide fournit des approches et des exemples pour automatiser les étapes manuelles (par exemple, l'installation et la configuration des agents, le suivi des métriques, la notification ou la prise de mesures en cas de problème). Ces approches sont utiles lorsque votre adoption du cloud arrive à maturité et augmente et que vous devez augmenter vos capacités opérationnelles sans augmenter les activités ou les ressources de gestion du cloud.

Planification de votre CloudWatch déploiement

La complexité et la portée d'une solution de journalisation et de surveillance dépendent de plusieurs facteurs, notamment :

- Combien d'environnements, de régions et de comptes sont utilisés et comment ce nombre pourrait augmenter.
- La variété et les types de vos charges de travail et architectures existantes.
- Les types de calcul et OSs ceux qui doivent être enregistrés et surveillés.
- S'il existe à la fois des sites et une AWS infrastructure sur site.
- Les exigences d'agrégation et d'analyse de plusieurs systèmes et applications.
- Exigences de sécurité qui empêchent l'exposition non autorisée de journaux et de mesures.
- Produits et solutions qui doivent s'intégrer à votre solution de journalisation et de surveillance pour soutenir les processus opérationnels.

Vous devez régulièrement revoir et mettre à jour votre solution de journalisation et de surveillance avec des déploiements de charge de travail nouveaux ou actualisés. Les mises à jour de votre journalisation, de votre surveillance et de vos alarmes doivent être identifiées et appliquées lorsque des problèmes sont observés. Ces problèmes peuvent ensuite être identifiés de manière proactive et évités à l'avenir.

Vous devez vous assurer que vous installez et configurez systématiquement les logiciels et les services permettant de capturer et d'ingérer les journaux et les mesures. Une approche de journalisation et de surveillance établie utilise des services et des solutions de fournisseurs de logiciels (ISV) multiples AWS ou indépendants pour différents domaines (par exemple, la sécurité, les performances, la mise en réseau ou l'analyse). Chaque domaine a ses propres exigences en matière de déploiement et de configuration.

Nous vous recommandons CloudWatch de l'utiliser pour capturer et ingérer des journaux et des métriques pour plusieurs OSs types de calcul. De nombreux AWS services sont utilisés CloudWatch pour enregistrer, surveiller et publier des journaux et des métriques, sans nécessiter de configuration supplémentaire. CloudWatch fournit un agent logiciel qui peut être installé et configuré pour différents OSs environnements. Les sections suivantes expliquent comment déployer, installer et configurer l' CloudWatch agent pour plusieurs comptes, régions et configurations :

Rubriques

Utilisation CloudWatch dans des comptes centralisés ou distribués

Bien qu' CloudWatch il soit conçu pour surveiller les AWS services ou les ressources d'un seul compte et d'une seule région, vous pouvez utiliser un compte central pour capturer les journaux et les statistiques de plusieurs comptes et régions. Si vous utilisez plusieurs comptes ou régions, vous devez déterminer s'il convient d'utiliser l'approche des comptes centralisés ou un compte individuel pour capturer les journaux et les statistiques. Généralement, une approche hybride est requise pour les déploiements multicomptes et multirégions afin de répondre aux exigences des responsables de la sécurité, de l'analyse, des opérations et de la charge de travail.

Le tableau suivant indique les points à prendre en compte lors du choix d'une approche centralisée, distribuée ou hybride.

Structures de comptes	Votre organisation peut avoir plusieurs comptes distincts (par exemple, des comptes pour les charges de travail hors productio n et de production) ou des milliers de comptes pour des applicati ons uniques dans des environnements spécifiques. Nous vous recommandons de conserver les journaux et les métriques des applications dans le compte sur lequel s'exécute la charge de travail, afin que les propriétaires de la charge de travail puissent accéder aux journaux et aux métriques. Cela leur permet de jouer un rôle actif dans la journalisation et la surveillance. Nous vous recommand ons également d'utiliser un compte de journalisation distinct pour agréger tous les journaux de charge de travail à des fins d'analyse , d'agrégation, de tendances et d'opérations centralisées. Des comptes de journalisation distincts peuvent également être utilisés pour la sécurité, l'archivage et la surveillance, ainsi que pour les analyses.
Exigences en matière d'accès	Les membres de l'équipe (par exemple, les propriétaires de charges de travail ou les développeurs) doivent avoir accès aux journaux

	et aux métriques pour résoudre les problèmes et apporter des améliorations. Les journaux doivent être conservés dans le compte de la charge de travail pour faciliter l'accès et le dépannage. Si les journaux et les métriques sont conservés dans un compte distinct de celui de la charge de travail, les utilisateurs peuvent avoir besoin d'alterner régulièrement entre les comptes. L'utilisation d'un compte centralisé fournit des informations de journal aux utilisateurs autorisés sans accorder l'accès au compte de charge de travail. Cela peut simplifier les exigences d'accès pour les charges de travail analytiques où l'agrégation est requise pour les charges de travail exécutées sur plusieurs comptes. Le compte de journalisation centralisé peut également proposer d'autres options de recherche et d'agrégation, telles qu'un cluster Amazon OpenSearch Service. Amazon OpenSearch Service fournit un contrôle d'accès précis jusqu'au niveau du terrain pour vos journaux. Un contrôle d'accès précis est important lorsque vous avez des données sensibles ou confidentielles qui nécessitent un accès et des autorisations spécialisés.
Opérations	De nombreuses organisations disposent d'une équipe centralisée chargée des opérations et de la sécurité ou d'une organisation externe chargée du support opérationnel qui a besoin d'accéder aux journaux à des fins de surveillance. La journalisation et la surveillance centralisées peuvent faciliter l'identification des tendances, la recherche, l'agrégation et l'exécution d'analyses sur tous les comptes et charges de travail. Si votre organisation utilise l'approche « vous le créez, vous l'exécutez » DevOps, les responsables de la charge de travail ont besoin de consigner et de surveiller les informations dans leur compte. Une approche hybride peut être nécessaire pour répondre aux besoins des opérations et des analyses centralisées, en plus de la propriété distribuée de la charge de travail.

Environnement	Vous pouvez choisir d'héberger les journaux et les métriques dans un emplacement central pour les comptes de production et de conserver les journaux et les métriques pour d'autres environnements (par exemple, le développement ou les tests) dans le même compte ou dans des comptes distincts, en fonction des exigences de sécurité et de l'architecture du compte. Cela permet d'empêcher un public plus large d'accéder aux données sensibles créées pendant la production.

CloudWatch propose plusieurs options pour traiter les journaux en temps réel grâce à des filtres CloudWatch d'abonnement. Vous pouvez utiliser des filtres d'abonnement pour diffuser les journaux en temps réel vers AWS des services à des fins de traitement, d'analyse et de chargement personnalisés vers d'autres systèmes. Cela peut être particulièrement utile si vous adoptez une approche hybride dans laquelle vos journaux et statistiques sont disponibles dans des comptes individuels et des régions, en plus d'un compte et d'une région centralisés. La liste suivante fournit des exemples de AWS services pouvant être utilisés à cette fin :

- Amazon Data Firehose — Firehose fournit une solution de streaming qui s'adapte et se redimensionne automatiquement en fonction du volume de données produit. Vous n'avez pas besoin de gérer le nombre de partitions dans un flux de données Amazon Kinesis et vous pouvez vous connecter directement à Amazon Simple Storage Service (Amazon S3) OpenSearch , Amazon Service ou Amazon Redshift sans codage supplémentaire. Firehose est une solution efficace si vous souhaitez centraliser vos logs dans ces services. AWS
- Amazon Kinesis Data Streams — Kinesis Data Streams est une solution appropriée si vous devez intégrer un service non pris en charge par Firehose et implémenter une logique de traitement supplémentaire. Vous pouvez créer une destination Amazon CloudWatch Logs dans vos comptes et régions qui spécifie un flux de données Kinesis dans un compte central et un rôle AWS Identity and Access Management (IAM) lui octroyant l'autorisation de placer des enregistrements dans le flux. Kinesis Data Streams fournit une zone d'atterrissage flexible et illimitée pour vos données de journal, qui peuvent ensuite être consommées par différentes options. Vous pouvez lire les données du journal Kinesis Data Streams dans votre compte, effectuer un prétraitement et envoyer les données vers la destination de votre choix.

  Cependant, vous devez configurer les partitions du flux de manière à ce qu'il soit correctement dimensionné pour les données de journal produites. Kinesis Data Streams agit comme un

intermédiaire ou une file d'attente temporaire pour vos données de journal, et vous pouvez stocker les données dans le flux Kinesis pendant un à 365 jours. Kinesis Data Streams prend également en charge la fonctionnalité de rediffusion, ce qui signifie que vous pouvez rejouer des données qui n'ont pas été consommées.

- Amazon OpenSearch Service — CloudWatch Logs peut diffuser les journaux d'un groupe de journaux vers un OpenSearch cluster via un compte individuel ou centralisé. Lorsque vous configurez un groupe de journaux pour diffuser des données vers un OpenSearch cluster, une fonction Lambda est créée dans le même compte et dans la même région que votre groupe de journaux. La fonction Lambda doit disposer d'une connexion réseau avec le OpenSearch cluster. Vous pouvez personnaliser la fonction Lambda pour effectuer un prétraitement supplémentaire, en plus de personnaliser l'ingestion dans Amazon Service. OpenSearch La journalisation centralisée avec Amazon OpenSearch Service facilite l'analyse, la recherche et le dépannage des problèmes liés aux multiples composants de votre architecture cloud.
- Lambda — Si vous utilisez Kinesis Data Streams, vous devez fournir et gérer les ressources de calcul qui consomment les données de votre flux. Pour éviter cela, vous pouvez transmettre les données du journal directement à Lambda pour traitement et les envoyer vers une destination en fonction de votre logique. Cela signifie que vous n'avez pas besoin de provisionner et de gérer des ressources informatiques pour traiter les données entrantes. Si vous choisissez d'utiliser Lambda, assurez-vous que votre solution est compatible avec les quotas Lambda.

Il se peut que vous deviez traiter ou partager des données de journal stockées dans CloudWatch des journaux au format de fichier. Vous pouvez créer une tâche d'exportation pour exporter un groupe de journaux vers Amazon S3 pour une date ou une plage horaire spécifique. Par exemple, vous pouvez choisir d'exporter les journaux quotidiennement vers Amazon S3 à des fins d'analyse et d'audit. Lambda peut être utilisé pour automatiser cette solution. Vous pouvez également associer cette solution à la réplication Amazon S3 pour expédier et centraliser vos journaux provenant de plusieurs comptes et régions vers un compte et une région centralisés.

La configuration de l' CloudWatch agent peut également spécifier un `credentials` champ dans la `agent`section. Cela indique un rôle IAM à utiliser lors de l'envoi de métriques et de journaux vers un autre compte. S'il est spécifié, ce champ contient le `role_arn` paramètre. Ce champ peut être utilisé lorsque vous n'avez besoin que d'une journalisation et d'une surveillance centralisées dans un compte centralisé et une région spécifiques.

Vous pouvez également utiliser le AWS SDK pour écrire votre propre application de traitement personnalisée dans la langue de votre choix, lire les journaux et les indicateurs de vos comptes et

envoyer des données vers un compte centralisé ou une autre destination pour un traitement et une surveillance ultérieurs.

Gestion des fichiers de configuration des CloudWatch agents

Nous vous recommandons de créer une configuration d' CloudWatch agent Amazon standard qui inclut les journaux système et les métriques que vous souhaitez capturer sur toutes vos instances Amazon Elastic Compute Cloud (Amazon EC2) et sur vos serveurs sur site. Vous pouvez utiliser l'assistant du fichier de configuration de l' CloudWatch agent pour vous aider à créer le fichier de configuration. Vous pouvez exécuter l'assistant de configuration plusieurs fois afin de générer des configurations uniques pour différents systèmes et environnements. Vous pouvez également modifier le fichier de configuration ou créer des variantes à l'aide du schéma du fichier de configuration. Le fichier de configuration de l' CloudWatch agent peut être stocké dans les paramètres d'AWS Systems Manager Parameter Store. Vous pouvez créer des paramètres de magasin de paramètres distincts si vous disposez de plusieurs fichiers de configuration d' CloudWatch agent. Si vous utilisez plusieurs comptes AWS ou régions AWS, vous devez gérer et mettre à jour les paramètres du magasin de paramètres dans chaque compte et région. Vous pouvez également gérer vos CloudWatch configurations de manière centralisée sous forme de fichiers dans Amazon S3 ou dans un outil de contrôle de version de votre choix.

Le `amazon-cloudwatch-agent-ctl` script inclus dans l' CloudWatch agent vous permet de spécifier un fichier de configuration, un paramètre Parameter Store ou la configuration par défaut de l'agent. La configuration par défaut s'aligne sur l'ensemble de mesures de base prédéfini et configure l'agent pour qu'il communique les métriques de mémoire et d'espace disque à. CloudWatch Cependant, il n'inclut aucune configuration de fichier journal. La configuration par défaut est également appliquée si vous utilisez la configuration rapide de Systems Manager pour l' CloudWatch agent.

Étant donné que la configuration par défaut n'inclut pas la journalisation et n'est pas personnalisée en fonction de vos besoins, nous vous recommandons de créer et d'appliquer vos propres CloudWatch configurations, personnalisées en fonction de vos besoins.

Gestion des CloudWatch configurations

Par défaut, les CloudWatch configurations peuvent être stockées et appliquées en tant que paramètres du magasin de paramètres ou en tant que fichiers CloudWatch de configuration. Le meilleur choix dépendra de vos besoins. Dans cette section, nous discutons des avantages et des

inconvénients de ces deux options. Une solution représentative est également détaillée pour gérer les fichiers CloudWatch de configuration pour plusieurs comptes AWS et régions AWS.

Paramètres du magasin de paramètres de Systems Manager

L'utilisation des paramètres du magasin de paramètres pour gérer les CloudWatch configurations fonctionne bien si vous avez un seul fichier de configuration d' CloudWatch agent standard que vous souhaitez appliquer et gérer dans un petit ensemble de comptes et de régions AWS. Lorsque vous stockez vos CloudWatch configurations sous forme de paramètres de magasin de paramètres, vous pouvez utiliser l'outil de configuration de l' CloudWatch agent (sous Linux) pour lire et appliquer la configuration depuis le magasin de paramètres sans avoir à copier le fichier de configuration `amazon-cloudwatch-agent-ctl` sur votre instance. Vous pouvez utiliser le document de commande AmazonCloudWatch- ManageAgent Systems Manager pour mettre à jour la CloudWatch configuration sur plusieurs EC2 instances en une seule exécution. Les paramètres du magasin de paramètres étant régionaux, vous devez mettre à jour et gérer les CloudWatch paramètres du magasin de paramètres dans chaque région AWS et chaque compte AWS. Si vous souhaitez appliquer plusieurs CloudWatch configurations à chaque instance, vous devez personnaliser le document AmazonCloudWatch- ManageAgent Command pour inclure ces paramètres.

CloudWatch fichiers de configuration

La gestion de vos CloudWatch configurations sous forme de fichiers peut fonctionner correctement si vous possédez de nombreux comptes et régions AWS et si vous gérez plusieurs fichiers CloudWatch de configuration. Grâce à cette approche, vous pouvez les parcourir, les organiser et les gérer dans une structure de dossiers. Vous pouvez appliquer des règles de sécurité à des dossiers ou à des fichiers individuels afin de limiter et d'accorder l'accès, par exemple des autorisations de mise à jour et de lecture. Vous pouvez les partager et les transférer en dehors d'AWS à des fins de collaboration. Vous pouvez contrôler les versions des fichiers pour suivre et gérer les modifications. Vous pouvez appliquer des CloudWatch configurations collectivement en copiant les fichiers de configuration dans le répertoire de configuration de l' CloudWatch agent sans appliquer chaque fichier de configuration individuellement. Pour Linux, le répertoire CloudWatch de configuration se trouve à l'adresse`/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d`. Pour Windows, le répertoire de configuration se trouve à l'adresse`C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs`.

Lorsque vous démarrez l' CloudWatch agent, celui-ci ajoute automatiquement chaque fichier présent dans ces répertoires pour créer un fichier de configuration CloudWatch composite. Les fichiers de configuration doivent être stockés dans un emplacement central (par exemple, un compartiment

S3) auquel les comptes et régions requis peuvent accéder. Un exemple de solution utilisant cette approche est fourni.

Organisation des CloudWatch configurations

Quelle que soit l'approche utilisée pour gérer vos CloudWatch configurations, CloudWatch organisez-les. Vous pouvez organiser vos configurations en chemins de fichier ou de magasin de paramètres en utilisant une approche telle que la suivante.

/config/standard/windows/ec2	Stockez les fichiers de CloudWatch configuration standard spécifiques à Windows pour Amazon. EC2 Vous pouvez également classer les configurations standard de votre système d'exploitation (OS) pour différentes versions de Windows, différents types d' EC2 instances et différents environnements dans ce dossier.
/config/standard/windows/onpremises	Stockez des fichiers de CloudWatch configuration standard spécifiques à Windows pour les serveurs locaux. Vous pouvez également classer plus en détail vos configurations de système d'exploitation standard pour les différentes versions de Windows, les différents types de serveurs et les différents environnements dans ce dossier.
/config/standard/linux/ec2	Stockez vos fichiers de CloudWatch configuration standard spécifiques à Linux pour Amazon. EC2 Vous pouvez également classer votre configuration de système d'exploitation standard pour différentes distributions Linux, types d' EC2 instances et environnements dans ce dossier.
/config/standard/linux/onpremises	Stockez vos fichiers de CloudWatch configuration standard spécifiques à Linux pour les serveurs locaux. Vous pouvez également classer votre configuration de système d'exploit

	ation standard pour différentes distributions Linux, types de serveurs et environnements dans ce dossier.
/config/ecs	Stockez les fichiers de CloudWatch configura tion spécifiques à Amazon Elastic Container Service (Amazon ECS) si vous utilisez des instances de conteneur Amazon ECS. Ces configurations peuvent être ajoutées aux EC2 configurations Amazon standard pour la journalisation et la surveillance au niveau des systèmes spécifiques à Amazon ECS.
/configuration/ <application_name>	Stockez les fichiers de CloudWatch configura tion spécifiques à votre application. Vous pouvez mieux classer vos applications à l'aide de dossiers et de préfixes supplémentaires pour les environnements et les versions.

Exemple : stockage des fichiers CloudWatch de configuration dans un compartiment S3

Cette section fournit un exemple d'utilisation d'Amazon S3 pour stocker les fichiers de CloudWatch configuration et un runbook personnalisé de Systems Manager pour récupérer et appliquer les fichiers CloudWatch de configuration. Cette approche permet de relever certains des défis liés à l'utilisation des paramètres du magasin de paramètres de Systems Manager pour une CloudWatch configuration à grande échelle :

- Si vous utilisez plusieurs régions, vous devez synchroniser les mises à jour CloudWatch de configuration dans le magasin de paramètres de chaque région. Parameter Store est un service régional et le même paramètre doit être mis à jour dans chaque région qui utilise l' CloudWatch agent.
- Si vous avez plusieurs CloudWatch configurations, vous devez lancer la récupération et l'application de chaque configuration du magasin de paramètres. Vous devez récupérer chaque CloudWatch configuration individuellement dans le magasin de paramètres et également mettre à jour la méthode de récupération chaque fois que vous ajoutez une nouvelle configuration.

En revanche, CloudWatch fournit un répertoire de configuration pour stocker les fichiers de configuration et applique chaque configuration du répertoire, sans qu'il soit nécessaire de les spécifier individuellement.

- Si vous utilisez plusieurs comptes, vous devez vous assurer que chaque nouveau compte possède les CloudWatch configurations requises dans son magasin de paramètres. Vous devez également vous assurer que toute modification de configuration sera appliquée à ces comptes et à leurs régions à l'avenir.

Vous pouvez stocker CloudWatch les configurations dans un compartiment S3 accessible depuis tous vos comptes et régions. Vous pouvez ensuite copier ces configurations depuis le compartiment S3 vers le répertoire de CloudWatch configuration à l'aide des runbooks Systems Manager Automation et de Systems Manager State Manager. Vous pouvez utiliser le modèle CloudFormation AWS cloudwatch-config-s3-bucket.yaml pour créer un compartiment S3 accessible depuis plusieurs comptes au sein d'une organisation dans AWS Organizations. Le modèle inclut un `OrganizationID` paramètre qui accorde un accès en lecture à tous les comptes de votre organisation.

L'exemple augmenté du runbook Systems Manager, fourni dans la section Set up State Manager and Distributor pour le déploiement et la configuration des CloudWatch agents de ce guide, est configuré pour récupérer des fichiers à l'aide du compartiment S3 créé par le modèle AWS cloudwatch-config-s3-bucket.yaml. CloudFormation

Vous pouvez également utiliser un système de contrôle de version (par exemple, GitHub) pour stocker vos fichiers de configuration. Si vous souhaitez récupérer automatiquement les fichiers de configuration stockés dans un système de contrôle de version, vous devez gérer ou centraliser le stockage des informations d'identification et mettre à jour le runbook Systems Manager Automation utilisé pour récupérer les informations d'identification sur vos comptes et. Régions AWS

Configuration de l' CloudWatch agent pour les EC2 instances et les serveurs locaux

De nombreuses entreprises exécutent des charges de travail à la fois sur des serveurs physiques et des machines virtuelles (VMs). Ces charges de travail s'exécutent généralement sur des serveurs différents, chacun OSs ayant des exigences d'installation et de configuration uniques pour la capture et l'ingestion de métriques.

Si vous choisissez d'utiliser EC2 des instances, vous pouvez avoir un haut niveau de contrôle sur la configuration de votre instance et de votre système d'exploitation. Toutefois, ce niveau supérieur de contrôle et de responsabilité vous oblige à surveiller et à ajuster les configurations pour une utilisation plus efficace. Vous pouvez améliorer votre efficacité opérationnelle en établissant des normes de journalisation et de surveillance, et en appliquant une approche d'installation et de configuration standard pour la capture et l'ingestion des journaux et des métriques.

Organisations qui migrent ou étendent leurs investissements informatiques vers le AWS cloud peuvent tirer parti CloudWatch d'une solution de journalisation et de surveillance unifiée. CloudWatch la tarification signifie que vous payez progressivement pour les statistiques et les journaux que vous souhaitez capturer. Vous pouvez également capturer des journaux et des métriques pour les serveurs sur site en utilisant un processus d'installation d' CloudWatch agent similaire à celui d'Amazon EC2.

Avant de commencer l'installation et le déploiement CloudWatch, assurez-vous d'évaluer les configurations de journalisation et de métrique de vos systèmes et applications. Assurez-vous de définir les journaux et les métriques standard que vous devez capturer pour OSs ce que vous souhaitez utiliser. Les journaux et les métriques du système constituent la base et la norme d'une solution de journalisation et de surveillance, car ils sont générés par le système d'exploitation et sont différents pour Linux et Windows. Des métriques et des fichiers journaux importants sont disponibles dans toutes les distributions Linux, en plus de ceux spécifiques à une version ou à une distribution Linux. Cette différence se produit également entre les différentes versions de Windows.

Configuration de l' CloudWatch agent

CloudWatch capture les métriques et les journaux pour Amazon EC2 et les serveurs locaux à l'aide d'CloudWatch agents et de fichiers de configuration d'agents spécifiques à chaque système d'exploitation. Nous vous recommandons de définir la configuration standard de capture des

métriques et des journaux de votre entreprise avant de commencer à installer l' CloudWatch agent à grande échelle dans vos comptes.

Vous pouvez combiner plusieurs configurations d' CloudWatch agent pour former une configuration d' CloudWatch agent composite. L'une des approches recommandées consiste à définir et à diviser les configurations de vos journaux et métriques au niveau du système et de l'application. Le schéma suivant montre comment plusieurs types CloudWatch de fichiers de configuration répondant à différentes exigences peuvent être combinés pour former une CloudWatch configuration composite :

Ces journaux et métriques peuvent également être mieux classés et configurés pour des environnements ou des exigences spécifiques. Par exemple, vous pouvez définir un sous-ensemble plus petit de journaux et de métriques avec une précision moindre pour les environnements de développement non réglementés, et un ensemble plus large et plus complet avec une précision supérieure pour les environnements de production réglementés.

Configuration de la capture du journal pour les EC2 instances

Par défaut, Amazon EC2 ne surveille ni ne capture les fichiers journaux. Au lieu de cela, les fichiers journaux sont capturés et ingérés dans les CloudWatch journaux par le logiciel CloudWatch agent installé sur votre EC2 instance, votre AWS API ou AWS Command Line Interface (AWS CLI). Nous vous recommandons d'utiliser l' CloudWatch agent pour ingérer les fichiers CloudWatch journaux dans Logs for Amazon EC2 et sur les serveurs locaux.

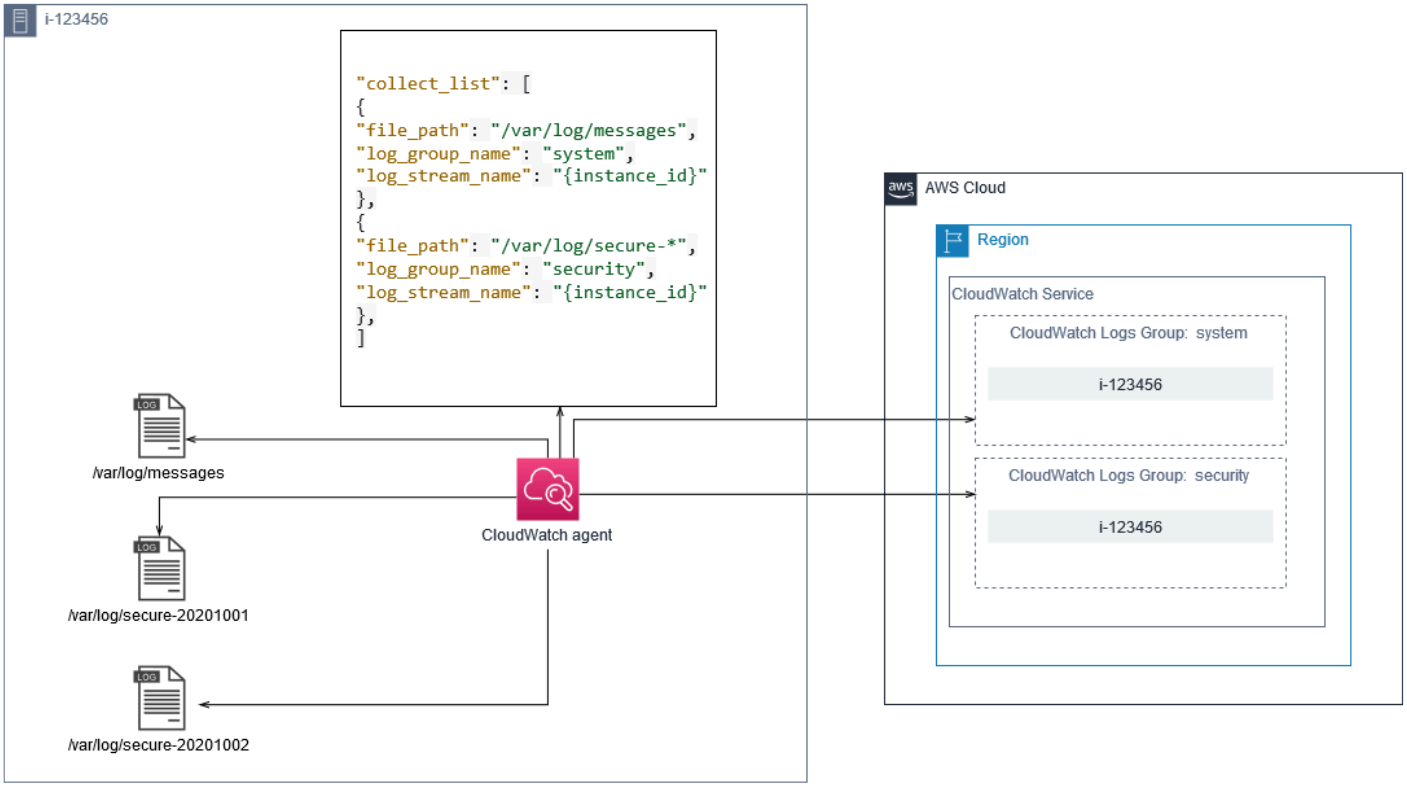
Vous pouvez rechercher et filtrer les journaux, extraire des métriques et exécuter l'automatisation en fonction de l'application de correctifs à partir des fichiers journaux. CloudWatch CloudWatch prend en charge les options de syntaxe de filtre et de modèle en texte brut, délimitées par des espaces et au format JSON, les journaux au format JSON offrant la plus grande flexibilité. Pour augmenter les options de filtrage et d'analyse, vous devez utiliser une sortie de journal formatée au lieu du texte brut.

L' CloudWatch agent utilise un fichier de configuration qui définit les journaux et les mesures à envoyer CloudWatch. CloudWatch capture ensuite chaque fichier journal sous forme de flux de journal et regroupe ces flux de journaux dans un groupe de journaux. Cela vous permet d'effectuer des opérations sur les journaux de vos EC2 instances, telles que la recherche d'une chaîne correspondante.

Le nom du flux de journal par défaut est identique à l'ID de l' EC2 instance et le nom du groupe de journaux par défaut est le même que le chemin du fichier journal. Le nom du flux de journaux

doit être unique au sein du groupe de CloudWatch journaux. Vous pouvez utiliser`instance_id`, `hostname``local_hostname`, ou `ip_address` pour une substitution dynamique dans les noms de flux de journaux et de groupes de journaux, ce qui signifie que vous pouvez utiliser le même fichier de configuration d' CloudWatch agent sur plusieurs EC2 instances.

Le schéma suivant montre la configuration d'un CloudWatch agent pour la capture des journaux. Le groupe de journaux est défini par les fichiers journaux capturés et contient des flux de journaux distincts pour chaque EC2 instance, car la `{instance_id}` variable est utilisée pour le nom du flux de journal et IDs les EC2 instances sont uniques.



Les groupes de journaux définissent la rétention, les balises, la sécurité, les filtres métriques et le champ de recherche des flux de journaux qu'ils contiennent. Le comportement de regroupement par défaut basé sur le nom du fichier journal vous permet de rechercher, de créer des métriques et d'émettre des alertes sur les données spécifiques à un fichier journal dans toutes les EC2 instances d'un compte et d'une région. Vous devez évaluer s'il est nécessaire d'affiner davantage les groupes de logs. Par exemple, votre compte peut être partagé par plusieurs unités commerciales et avoir différents responsables techniques ou opérationnels. Cela signifie que vous devez affiner davantage le nom du groupe de journaux pour refléter la séparation et la propriété. Cette approche vous permet de concentrer votre analyse et votre résolution des problèmes sur l' EC2 instance appropriée.

Si plusieurs environnements utilisent un seul compte, vous pouvez séparer la journalisation des charges de travail exécutées dans chaque environnement. Le tableau suivant présente une convention de dénomination des groupes de journaux qui inclut l'unité commerciale, le projet ou l'application et l'environnement.

Nom du groupe de journaux	`/<Business unit>/<Project or application name>/<Environment>/<Log file name>`
Nom du flux de log	`<EC2 instance ID>`

Vous pouvez également regrouper tous les fichiers journaux d'une EC2 instance dans le même groupe de journaux. Cela facilite la recherche et l'analyse dans un ensemble de fichiers journaux pour une seule EC2 instance. Cela est utile si la plupart de vos EC2 instances ne desservent qu'une seule application ou charge de travail et que chaque EC2 instance répond à un objectif spécifique. Le tableau suivant montre comment le nom de votre groupe de journaux et de votre flux de journaux peut être formaté pour prendre en charge cette approche.

Nom du groupe de journaux	`/<Business unit>/<Project or application name>/<Environment>/<EC2 instance ID>`
Nom du flux de log	`<Log file name>`

Configuration de la capture des métriques pour les EC2 instances

Par défaut, vos EC2 instances sont activées pour la surveillance de base et un ensemble standard de mesures (par exemple, des mesures relatives au processeur, au réseau ou au stockage) est automatiquement envoyé CloudWatch toutes les cinq minutes. CloudWatch les métriques peuvent varier en fonction de la famille d'instances. Par exemple, les instances de performance burstable disposent de métriques pour les crédits CPU. Les métriques EC2 standard d'Amazon sont incluses dans le prix de votre instance. Si vous activez la surveillance détaillée de vos EC2 instances, vous pouvez recevoir des données par périodes d'une minute. La fréquence des périodes a un impact sur vos CloudWatch coûts. Assurez-vous donc d'évaluer si un suivi détaillé est requis pour toutes

vos EC2 instances ou uniquement pour certaines d'entre elles. Par exemple, vous pouvez activer la surveillance détaillée des charges de travail de production, mais utiliser la surveillance de base pour les charges de travail hors production.

Les serveurs locaux n'incluent aucune métrique par défaut CloudWatch et doivent utiliser l' CloudWatch agent ou le AWS CLI AWS SDK pour capturer les métriques. Cela signifie que vous devez définir les métriques que vous souhaitez capturer (par exemple, l'utilisation du processeur) dans le fichier CloudWatch de configuration. Vous pouvez créer un fichier CloudWatch de configuration unique qui inclut les métriques d' EC2 instance standard pour vos serveurs locaux et l'appliquer en plus de votre CloudWatch configuration standard.

Les métriques entrées CloudWatch sont définies de manière unique par le nom de la métrique et par zéro dimension ou plus, et sont regroupées de manière unique dans un espace de noms de métrique. Les métriques fournies par un AWS service ont un espace de noms qui commence par `AWS` (par exemple,`AWS/EC2`), et les mesures non AWS métriques sont considérées comme des métriques personnalisées. Les métriques que vous configurez et capturez avec l' CloudWatch agent sont toutes considérées comme des métriques personnalisées. Le nombre de métriques créées ayant un impact sur vos CloudWatch coûts, vous devez déterminer si chaque métrique est requise pour toutes vos EC2 instances ou uniquement pour certaines d'entre elles. Par exemple, vous pouvez définir un ensemble complet de mesures pour les charges de travail de production, mais utiliser un sous-ensemble plus restreint de ces mesures pour les charges de travail hors production.

`CWAgent`est l'espace de noms par défaut pour les métriques publiées par l' CloudWatch agent. À l'instar des groupes de journaux, l'espace de noms des métriques organise un ensemble de métriques afin qu'elles puissent être trouvées ensemble au même endroit. Vous devez modifier l'espace de noms pour qu'il reflète une unité commerciale, un projet ou une application, ainsi qu'un environnement (par exemple,`/<Business unit>/<Project or application name>/<Environment>`). Cette approche est utile si plusieurs charges de travail indépendantes utilisent le même compte. Vous pouvez également corréler la convention de dénomination de votre espace de nommage à la convention de dénomination de votre groupe de CloudWatch journaux.

Les métriques sont également identifiées par leurs dimensions, ce qui vous permet de les analyser par rapport à un ensemble de conditions. Ce sont les propriétés par rapport auxquelles les observations sont enregistrées. Amazon EC2 inclut des statistiques distinctes pour les EC2 instances avec `InstanceId` et pour `AutoScalingGroupName` les dimensions. Vous recevez également des métriques avec les `InstanceType` dimensions `ImageId` et si vous activez le suivi détaillé. Par exemple, Amazon EC2 fournit une métrique d' EC2 instance distincte pour l'utilisation du processeur avec les `InstanceId` dimensions, en plus d'une métrique d'utilisation du processeur distincte pour la

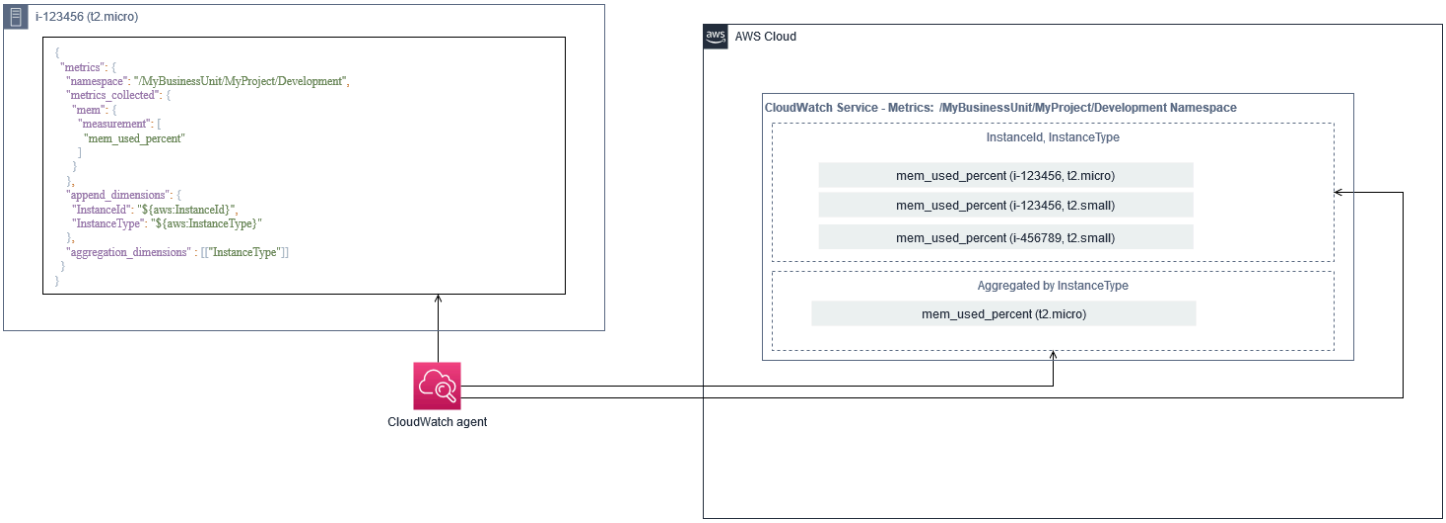
`InstanceType` dimension. Cela vous permet d'analyser l'utilisation du processeur pour chaque EC2 instance unique, en plus de toutes les EC2 instances d'un type d'instance spécifique.

L'ajout de dimensions augmente votre capacité d'analyse mais augmente également vos coûts globaux, car chaque combinaison de mesures et de valeurs de dimension uniques donne lieu à une nouvelle métrique. Par exemple, si vous créez une métrique pour le pourcentage d'utilisation de la mémoire par rapport à la `InstanceId` dimension, il s'agit d'une nouvelle métrique pour chaque EC2 instance. Si votre organisation gère des milliers d' EC2 instances, cela génère des milliers de métriques et entraîne une hausse des coûts. Pour contrôler et prévoir les coûts, assurez-vous de déterminer la cardinalité de la métrique et les dimensions qui ajoutent le plus de valeur. Par exemple, vous pouvez définir un ensemble complet de dimensions pour les mesures de votre charge de travail de production, mais un sous-ensemble plus restreint de ces dimensions pour les charges de travail hors production.

Vous pouvez utiliser cette `append_dimensions` propriété pour ajouter des dimensions à une ou à toutes les métriques définies dans votre CloudWatch configuration. Vous pouvez également ajouter dynamiquement le`ImageId`, `InstanceIdInstanceType`, et `AutoScalingGroupName` à toutes les métriques de votre CloudWatch configuration. Vous pouvez également ajouter un nom et une valeur de dimension arbitraires pour des métriques spécifiques en utilisant la `append_dimensions` propriété de cette métrique. CloudWatch peut également agréger des statistiques sur les dimensions métriques que vous avez définies avec la `aggregation_dimensions` propriété.

Par exemple, vous pouvez agréger la mémoire utilisée par rapport à la `InstanceType` dimension pour voir la mémoire moyenne utilisée par toutes les EC2 instances pour chaque type d'instance. Si vous utilisez `t2.micro` des instances exécutées dans une région, vous pouvez déterminer si les charges de travail utilisant la `t2.micro` classe surutilisent ou sous-utilisent la mémoire fournie. La sous-utilisation peut être le signe que les charges de travail utilisent des EC2 classes dont la capacité de mémoire n'est pas requise. En revanche, la surutilisation peut être le signe de charges de travail utilisant des EC2 classes Amazon avec une mémoire insuffisante.

Le schéma suivant montre un exemple de configuration de CloudWatch métriques qui utilise un espace de noms personnalisé, des dimensions ajoutées et une agrégation par`InstanceType`.



Configuration au niveau du CloudWatch système

Les métriques et les journaux au niveau du système constituent un élément central d'une solution de surveillance et de journalisation, et l' CloudWatch agent dispose d'options de configuration spécifiques pour Windows et Linux.

Nous vous recommandons d'utiliser l'assistant de fichier CloudWatch de configuration ou le schéma du fichier de configuration pour définir le fichier de configuration de l' CloudWatch agent pour chaque système d'exploitation que vous envisagez de prendre en charge. Des journaux et des métriques supplémentaires spécifiques à la charge de travail au niveau du système d'exploitation peuvent être définis dans des fichiers de CloudWatch configuration distincts et ajoutés à la configuration standard. Ces fichiers de configuration uniques doivent être stockés séparément dans un compartiment S3 où ils peuvent être récupérés par vos EC2 instances. Un exemple de configuration d'un compartiment S3 à cette fin est décrit dans la Gestion des CloudWatch configurations section de ce guide. Vous pouvez récupérer et appliquer automatiquement ces configurations à l'aide de State Manager et de Distributor.

Configuration des journaux au niveau du système

Les journaux au niveau du système sont essentiels pour diagnostiquer et résoudre les problèmes sur site ou dans le cloud. AWS Votre approche de capture des journaux doit inclure tous les journaux système et de sécurité générés par le système d'exploitation. Les fichiers journaux générés par le système d'exploitation peuvent être différents selon la version du système d'exploitation.

L' CloudWatch agent prend en charge la surveillance des journaux d'événements Windows en fournissant le nom du journal d'événements. Vous pouvez choisir les journaux d'événements Windows que vous souhaitez surveiller (par exemple `SystemApplication`, ou`Security`).

Les journaux du système, des applications et de sécurité des systèmes Linux sont généralement stockés dans le `/var/log` répertoire. Le tableau suivant définit les fichiers journaux par défaut courants que vous devez surveiller, mais vous devez vérifier le `/etc/syslog.conf` fichier `/etc/rsyslog.conf` ou pour déterminer la configuration spécifique des fichiers journaux de votre système.

Diffusion de Fedora (Amazon Linux, CentOS, Red Hat Enterprise Linux)	`/var/log/boot.log*` — Journal de démarrage
	`/var/log/dmesg` — Journal du noyau
	`/var/log/secure` — Journal de sécurité et d'authentification
	`/var/log/messages` — Journal général du système
	`/var/log/cron*` — Journaux Cron
	`/var/log/cloud-init-output.log` — Résultat des scripts de `Userdata` démarrage
Debian (Ubuntu)	`/var/log/syslog` — Journal de démarrage
	`/var/log/cloud-init-output.log` — Résultat des scripts de `Userdata` démarrage
	`/var/log/auth.log` — Journal de sécurité et d'authentification
	`/var/log/kern.log` — Journal du noyau

Votre organisation peut également disposer d'autres agents ou composants du système qui génèrent des journaux que vous souhaitez surveiller. Vous devez évaluer et décider quels fichiers journaux

sont générés par ces agents ou applications, et les inclure dans votre configuration en identifiant leur emplacement. Par exemple, vous devez inclure le Systems Manager et les journaux des CloudWatch agents dans votre configuration. Le tableau suivant indique l'emplacement de ces journaux d'agent pour Windows et Linux.

Windows	CloudWatch agent	`$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log`

	Agent 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	CloudWatch agent	`/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log`

	Agent 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`

CloudWatch ignore un fichier journal si celui-ci est défini dans la configuration de l' CloudWatch agent mais n'est pas trouvé. Cela est utile lorsque vous souhaitez conserver une configuration de journal unique pour Linux, plutôt que des configurations distinctes pour chaque distribution. C'est également utile lorsqu'un fichier journal n'existe pas tant que l'agent ou l'application logicielle ne démarre pas.

Configuration des métriques au niveau du système

L'utilisation de la mémoire et de l'espace disque n'est pas incluse dans les statistiques standard fournies par Amazon EC2. Pour inclure ces métriques, vous devez installer et configurer l' CloudWatch agent sur vos EC2 instances. L'assistant de configuration de l' CloudWatch agent crée une CloudWatch configuration avec des métriques prédéfinies et vous pouvez ajouter ou supprimer des métriques selon vos besoins. Assurez-vous de passer en revue les ensembles de mesures prédéfinis pour déterminer le niveau approprié dont vous avez besoin.

Les utilisateurs finaux et les responsables de la charge de travail doivent publier des métriques système supplémentaires en fonction des exigences spécifiques d'un serveur ou d'une EC2 instance. Ces définitions de métriques doivent être stockées, versionnées et gérées dans un fichier de configuration d' CloudWatch agent distinct, puis partagées dans un emplacement central (par exemple, Amazon S3) à des fins de réutilisation et d'automatisation.

Les EC2 métriques Amazon standard ne sont pas automatiquement capturées sur les serveurs locaux. Ces métriques doivent être définies dans un fichier de configuration d' CloudWatch agent utilisé par les instances locales. Vous pouvez créer un fichier de configuration de métriques distinct pour les instances locales avec des métriques telles que l'utilisation du processeur, et ajouter ces métriques au fichier de configuration de métriques standard.

Configuration au niveau de l'application CloudWatch

Les journaux et les métriques des applications sont générés par les applications en cours d'exécution et sont spécifiques aux applications. Assurez-vous de définir les journaux et les mesures nécessaires pour surveiller de manière adéquate les applications régulièrement utilisées par votre organisation. Par exemple, votre organisation a peut-être standardisé les applications Web sur Microsoft Internet Information Server (IIS). Vous pouvez créer une CloudWatch configuration standard de log et de métrique pour IIS qui peut également être utilisée dans l'ensemble de votre organisation. Les fichiers de configuration spécifiques à l'application peuvent être stockés dans un emplacement centralisé (par exemple, un compartiment S3) et sont accessibles par les propriétaires de charge de travail ou via une récupération automatique, puis copiés dans le CloudWatch répertoire de configuration. L' CloudWatch agent combine automatiquement les fichiers de CloudWatch configuration présents dans

le répertoire des fichiers de configuration de chaque EC2 instance ou serveur dans une CloudWatch configuration composite. Le résultat final est une CloudWatch configuration qui inclut la configuration standard au niveau du système de votre entreprise, ainsi que toutes les configurations pertinentes au niveau de l'application CloudWatch .

Les propriétaires de charges de travail doivent identifier et configurer les fichiers journaux et les mesures pour tous les composants et applications critiques.

Configuration des journaux au niveau de l'application

La journalisation au niveau de l'application varie selon qu'il s'agit d'une application commerciale off-the-shelf (COTS) ou d'une application développée sur mesure. Les applications COTS et leurs composants peuvent fournir plusieurs options pour la configuration et la sortie des journaux, telles que le niveau de détail du journal, le format du fichier journal et l'emplacement du fichier journal. Cependant, la plupart des applications COTS ou tierces ne vous permettent pas de modifier fondamentalement la journalisation (par exemple, en mettant à jour le code de l'application pour inclure des instructions de journal supplémentaires ou des formats non configurables). Vous devez au minimum configurer les options de journalisation pour les applications COTS ou tierces afin de consigner les informations relatives aux avertissements et aux erreurs, de préférence au format JSON.

Vous pouvez intégrer des applications développées sur mesure à CloudWatch Logs en incluant les fichiers journaux de l'application dans votre CloudWatch configuration. Les applications personnalisées améliorent la qualité et le contrôle des journaux, car vous pouvez personnaliser le format de sortie des journaux, classer et séparer les sorties des composants pour séparer les fichiers journaux, en plus d'inclure les informations supplémentaires requises. Assurez-vous de passer en revue et de normaliser les bibliothèques de journalisation ainsi que les données et le formatage requis pour votre organisation afin de faciliter les analyses et le traitement.

Vous pouvez également écrire dans un flux de CloudWatch journal à l'aide de l'appel de `PutLogEvents` l'API CloudWatch Logs ou à l'aide du AWS SDK. Vous pouvez utiliser l'API ou le SDK pour des exigences de journalisation personnalisées, telles que la coordination de la journalisation dans un flux de journal unique sur un ensemble distribué de composants et de serveurs. Cependant, la solution la plus simple à gérer et la plus largement applicable consiste à configurer vos applications pour qu'elles écrivent dans des fichiers journaux, puis à utiliser l' CloudWatch agent pour lire les fichiers journaux et les diffuser en continu CloudWatch.

Vous devez également prendre en compte le type de métriques que vous souhaitez mesurer à partir des fichiers journaux de votre application. Vous pouvez utiliser des filtres métriques pour

mesurer, représenter graphiquement et générer des alarmes sur ces données dans un groupe de CloudWatch journaux. Par exemple, vous pouvez utiliser un filtre métrique pour compter les tentatives de connexion infructueuses en les identifiant dans vos journaux.

Vous pouvez également créer des métriques personnalisées pour vos applications développées sur mesure en utilisant le format de métrique CloudWatch intégré dans les fichiers journaux de vos applications.

Configuration des métriques au niveau de l'application

Les métriques personnalisées sont des métriques qui ne sont pas directement fournies par les AWS services à CloudWatch et elles sont publiées dans un espace de noms personnalisé dans CloudWatch les métriques. Toutes les métriques d'application sont considérées comme des CloudWatch métriques personnalisées. Les métriques d'application peuvent s'aligner sur une EC2 instance, un composant d'application, un appel d'API ou même une fonction métier. Vous devez également tenir compte de l'importance et de la cardinalité des dimensions que vous choisissez pour vos indicateurs. Les dimensions présentant une cardinalité élevée génèrent un grand nombre de mesures personnalisées et peuvent augmenter vos CloudWatch coûts.

CloudWatch vous permet de capturer des métriques au niveau de l'application de plusieurs manières, notamment de la manière suivante :

- Capturez les métriques au niveau des processus en définissant les processus individuels que vous souhaitez capturer à partir du plugin procstat.
- Une application publie une métrique dans Windows Performance Monitor et cette métrique est définie dans la CloudWatch configuration.
- Les filtres et modèles métriques sont appliqués aux connexions d'une application CloudWatch.
- Une application écrit dans un CloudWatch journal en utilisant le format métrique CloudWatch intégré.
- Une application envoie une métrique CloudWatch via l'API ou le AWS SDK.
- Une application envoie une métrique à un démon collectd ou StatsD avec un agent configuré. CloudWatch

Vous pouvez utiliser procstat pour surveiller et mesurer les processus applicatifs critiques avec l' CloudWatchagent. Cela vous permet de déclencher une alarme et de prendre des mesures (par exemple, une notification ou un processus de redémarrage) si un processus critique n'est plus en

cours d'exécution pour votre application. Vous pouvez également mesurer les caractéristiques de performance des processus de votre application et déclencher une alarme si un processus particulier agit de manière anormale.

La surveillance Procstat est également utile si vous ne pouvez pas mettre à jour vos applications COTS avec des métriques personnalisées supplémentaires. Par exemple, vous pouvez créer une `my_process` métrique qui mesure `cpu_time` et inclut une `application_version` dimension personnalisée. Vous pouvez également utiliser plusieurs fichiers de configuration d' CloudWatch agent pour une application si vous avez des dimensions différentes pour différents indicateurs.

Si votre application s'exécute sous Windows, vous devez évaluer si elle publie déjà des statistiques dans Windows Performance Monitor. De nombreuses applications COTS s'intègrent à Windows Performance Monitor, qui vous permet de surveiller facilement les indicateurs des applications. CloudWatch s'intègre également à Windows Performance Monitor et vous pouvez capturer toutes les mesures qui y sont déjà disponibles.

Assurez-vous de vérifier le format de journalisation et les informations de journal fournies par vos applications afin de déterminer quelles mesures peuvent être extraites à l'aide de filtres métriques. Vous pouvez consulter les journaux historiques de l'application afin de déterminer comment les messages d'erreur et les arrêts anormaux sont représentés. Vous devez également examiner les problèmes signalés précédemment afin de déterminer si une métrique peut être capturée afin d'éviter que le problème ne se reproduise. Vous devez également consulter la documentation de l'application et demander aux développeurs de l'application de confirmer comment les messages d'erreur peuvent être identifiés.

Pour les applications développées sur mesure, collaborez avec les développeurs de l'application pour définir les mesures importantes qui peuvent être mises en œuvre à l'aide du format de métrique CloudWatch intégré, du AWS SDK ou AWS de l'API. L'approche recommandée consiste à utiliser le format métrique intégré. Vous pouvez utiliser les bibliothèques de formats métriques intégrées open source AWS fournies pour vous aider à rédiger vos instructions dans le format requis. Vous devez également mettre à jour la CloudWatch configuration spécifique à votre application pour inclure l'agent de format métrique intégré. Cela fait en sorte que l'agent exécuté sur l' EC2 instance agit comme un point de terminaison local au format métrique intégré qui envoie des métriques au format métrique intégré à CloudWatch.

Si vos applications prennent déjà en charge la publication de métriques à collecter ou à indiquer, vous pouvez les exploiter pour y investir des métriques. CloudWatch

CloudWatch approches d'installation d'agents pour Amazon EC2 et les serveurs sur site

L'automatisation du processus d'installation de l' CloudWatch agent vous permet de le déployer rapidement et de manière cohérente et de capturer les journaux et les indicateurs requis. Il existe plusieurs approches pour automatiser l'installation de l' CloudWatch agent, notamment la prise en charge de plusieurs comptes et de plusieurs régions. Les approches d'installation automatisée suivantes sont abordées :

- Installation de l' CloudWatch agent à l'aide de Systems Manager Distributor et de Systems Manager State Manager : nous vous recommandons d'utiliser cette approche si vos EC2 instances et vos serveurs locaux exécutent l'agent Systems Manager. Cela garantit que l' CloudWatch agent est maintenu à jour et que vous pouvez créer des rapports sur les serveurs qui ne disposent pas de l' CloudWatch agent et y remédier. Cette approche s'adapte également pour prendre en charge plusieurs comptes et régions.
- Déploiement de l' CloudWatch agent dans le cadre du script de données utilisateur lors du provisionnement de l' EC2 instance : Amazon vous EC2 permet de définir un script de démarrage qui est exécuté lors du premier démarrage ou du premier redémarrage. Vous pouvez définir un script pour automatiser le processus de téléchargement et d'installation de l'agent. Cela peut également être inclus dans les CloudFormation scripts et les produits AWS Service Catalog. Cette approche peut être appropriée selon les besoins s'il existe une approche personnalisée d'installation et de configuration de l'agent pour une charge de travail spécifique qui s'écarte de vos normes.
- Inclure l' CloudWatchagent dans Amazon Machine Images (AMIs) — Vous pouvez installer l' CloudWatchagent dans votre version personnalisée AMIs pour Amazon EC2. Les EC2 instances qui utilisent l'AMI installeront et démarreront automatiquement l'agent. Cependant, vous devez vous assurer que l'agent et sa configuration sont régulièrement mis à jour.

Installation de l' CloudWatch agent à l'aide de Systems Manager Distributor et State Manager

Vous pouvez utiliser Systems Manager State Manager avec Systems Manager Distributor pour installer et mettre à jour automatiquement l' CloudWatch agent sur les serveurs et les EC2 instances.

Le distributeur inclut le package `AmazonCloudWatchAgent` AWS géré qui installe la version la plus récente de CloudWatch l'agent.

Cette approche d'installation comporte les prérequis suivants :

- L'agent Systems Manager doit être installé et exécuté sur vos serveurs ou EC2 instances. L'agent Systems Manager est préinstallé sur Amazon Linux, Amazon Linux 2, etc. AMIs L'agent doit également être installé et configuré sur d'autres images ou sur site VMs et sur des serveurs.

  > **Note**
  >
  > Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs.

- Un rôle IAM ou des informations d'identification disposant des autorisations requises CloudWatch et de Systems Manager doivent être attachés à l' EC2 instance ou définis dans le fichier d'informations d'identification d'un serveur sur site. Par exemple, vous pouvez créer un rôle IAM qui inclut les politiques AWS gérées : `AmazonSSMManagedInstanceCore` pour Systems Manager et `CloudWatchAgentServerPolicy` pour CloudWatch. Vous pouvez utiliser le CloudFormation modèle ssm-cloudwatch-instance-role.yaml pour déployer un rôle IAM et un profil d'instance qui incluent ces deux politiques. Ce modèle peut également être modifié pour inclure d'autres autorisations IAM standard pour vos EC2 instances. Pour les serveurs locaux ou VMs si vous devez configurer l' CloudWatch agent pour qu'il utilise le rôle de service Systems Manager configuré pour le serveur local. Pour plus d'informations à ce sujet, consultez Comment configurer les serveurs locaux qui utilisent l'agent Systems Manager et l' CloudWatch agent unifié pour n'utiliser que des informations d'identification temporaires ? dans le AWS Knowledge Center.

La liste suivante présente plusieurs avantages liés à l'utilisation de l'approche Systems Manager Distributor et State Manager pour installer et gérer l' CloudWatch agent :

- Installation automatisée pour plusieurs OSs : il n'est pas nécessaire d'écrire et de gérer un script pour chaque système d'exploitation afin de télécharger et d'installer l' CloudWatchagent.
- Contrôles de mise à jour automatiques : State Manager vérifie automatiquement et régulièrement que chaque EC2 instance dispose de la CloudWatch version la plus récente.
- Rapports de conformité : le tableau de bord de conformité de Systems Manager indique EC2 les instances qui n'ont pas réussi à installer le package Distributor.

- Installation automatisée pour les EC2 instances nouvellement lancées : EC2 les nouvelles instances lancées sur votre compte reçoivent automatiquement l' CloudWatch agent.

Toutefois, vous devez également tenir compte des trois points suivants avant de choisir cette approche :

- Collision avec une association existante : si une autre association installe ou configure déjà l' CloudWatch agent, les deux associations risquent d'interférer l'une avec l'autre et de provoquer des problèmes. Lorsque vous utilisez cette approche, vous devez supprimer toutes les associations existantes qui installent ou mettent à jour l' CloudWatchagent et la configuration.
- Mise à jour des fichiers de configuration d'agent personnalisés : le distributeur effectue une installation en utilisant le fichier de configuration par défaut. Si vous utilisez un fichier de configuration personnalisé ou plusieurs fichiers CloudWatch de configuration, vous devez mettre à jour la configuration après l'installation.
- Configuration multirégionale ou multicompte — L'association State Manager doit être configurée dans chaque compte et région. Les nouveaux comptes dans un environnement multi-comptes doivent être mis à jour pour inclure l'association State Manager. Vous devez centraliser ou synchroniser la CloudWatch configuration afin que plusieurs comptes et régions puissent récupérer et appliquer les normes requises.

Configurer State Manager et Distributor pour le déploiement et la configuration des CloudWatch agents

Vous pouvez utiliser la configuration rapide de Systems Manager pour configurer rapidement les fonctionnalités de Systems Manager, notamment en installant et en mettant à jour automatiquement l' CloudWatch agent sur vos EC2 instances. La configuration rapide déploie une CloudFormation pile qui déploie et configure les ressources de Systems Manager en fonction de vos choix.

La liste suivante fournit deux actions importantes effectuées par Quick Setup pour l'installation et la mise à jour automatisées des CloudWatch agents :

1. Créer des documents personnalisés de Systems Manager — Quick Setup crée les documents Systems Manager suivants à utiliser avec State Manager. Les noms des documents peuvent varier, mais le contenu reste le même :
   - `CreateAndAttachIAMToInstance`— Crée le profil de `AmazonSSMRoleForInstancesQuickSetup` rôle et d'instance s'ils n'existent pas et

attache la `AmazonSSMManagedInstanceCore` politique au rôle. Cela n'inclut pas la politique `CloudWatchAgentServerPolicy` IAM requise. Vous devez mettre à jour cette politique et mettre à jour ce document Systems Manager pour inclure cette politique, comme décrit dans la section suivante.

- `InstallAndManageCloudWatchDocument`— Installe l' CloudWatch agent avec Distributor et configure chaque EC2 instance une fois avec une configuration d' CloudWatch agent par défaut à l'aide du document `AWS-ConfigureAWSPackage` Systems Manager.
- `UpdateCloudWatchDocument`— Met à jour l' CloudWatch agent en installant le dernier CloudWatch agent à l'aide du document `AWS-ConfigureAWSPackage` Systems Manager. La mise à jour ou la désinstallation de l'agent ne supprime pas les fichiers de CloudWatch configuration existants de l' EC2 instance.

2. Créer des associations State Manager : les associations State Manager sont créées et configurées pour utiliser les documents Systems Manager créés sur mesure. Les noms des associations State Manager peuvent varier, mais la configuration reste la même :
   - `ManageCloudWatchAgent`— Exécute le document `InstallAndManageCloudWatchDocument` Systems Manager une fois pour chaque EC2 instance.
   - `UpdateCloudWatchAgent`— Exécute le document `UpdateCloudWatchDocument` Systems Manager tous les 30 jours pour chaque EC2 instance.
   - Exécute le document `CreateAndAttachIAMToInstance` Systems Manager une fois pour chaque EC2 instance.

Vous devez augmenter et personnaliser la configuration de configuration rapide terminée pour inclure CloudWatch les autorisations et prendre en charge les CloudWatch configurations personnalisées. En particulier, le document `CreateAndAttachIAMToInstance` et le `InstallAndManageCloudWatchDocument` document devront être mis à jour. Vous pouvez mettre à jour manuellement les documents Systems Manager créés par Quick Setup. Vous pouvez également utiliser votre propre CloudFormation modèle pour fournir les mêmes ressources avec les mises à jour nécessaires, ainsi que pour configurer et déployer d'autres ressources de Systems Manager sans utiliser Quick Setup.

> **Important**
>
> Quick Setup crée une CloudFormation pile pour déployer et configurer les ressources de Systems Manager en fonction de vos choix. Si vous mettez à jour vos choix de configuration

rapide, vous devrez peut-être mettre à jour à nouveau manuellement les documents de Systems Manager.

Les sections suivantes décrivent comment mettre à jour manuellement les ressources de Systems Manager créées par Quick Setup, ainsi que comment utiliser votre propre CloudFormation modèle pour effectuer une mise à jour de Quick Setup. Nous vous recommandons d'utiliser votre propre CloudFormation modèle pour éviter de mettre à jour manuellement les ressources créées par Quick Setup et CloudFormation.

Utilisez la configuration rapide de Systems Manager et mettez à jour manuellement les ressources Systems Manager créées

Les ressources Systems Manager créées par l'approche Quick Setup doivent être mises à jour pour inclure les autorisations d' CloudWatch agent requises et prendre en charge plusieurs fichiers CloudWatch de configuration. Cette section décrit comment mettre à jour le rôle IAM et les documents de Systems Manager afin d'utiliser un compartiment S3 centralisé contenant des CloudWatch configurations accessibles depuis plusieurs comptes. La création d'un compartiment S3 pour stocker les fichiers de CloudWatch configuration est décrite dans la Gestion des CloudWatch configurations section de ce guide.

Mettre à jour le document **`CreateAndAttachIAMToInstance`** Systems Manager

Ce document Systems Manager créé par Quick Setup vérifie si un profil d' EC2 instance IAM existant est attaché à une instance. Si c'est le cas, il associe la `AmazonSSMManagedInstanceCore` politique au rôle existant. Cela protège vos EC2 instances existantes contre la perte des AWS autorisations qui pourraient être attribuées par le biais de profils d'instance existants. Vous devez ajouter une étape dans ce document pour associer la politique `CloudWatchAgentServerPolicy` IAM aux EC2 instances auxquelles un profil d'instance est déjà attaché. Le document Systems Manager crée également le rôle IAM s'il n'existe pas et qu'aucun profil d' EC2 instance n'est associé à une instance. Vous devez mettre à jour cette section du document pour inclure également la politique `CloudWatchAgentServerPolicy` IAM.

Passez en revue le document CreateAndAttachIAMTod'exemple Instance.yaml terminé et comparez-le au document créé par Quick Setup. Modifiez le document existant pour inclure les étapes et les modifications requises. En fonction de vos choix de configuration rapide, le document créé par Configuration rapide peut être différent de l'exemple de document fourni. Veillez donc à effectuer les

ajustements nécessaires. L'exemple de document inclut l'option Quick Setup qui permet de scanner quotidiennement les instances pour détecter les correctifs manquants et inclut donc une politique pour le gestionnaire de correctifs de Systems Manager.

Mettre à jour le document **`InstallAndManageCloudWatchDocument`** Systems Manager

Ce document Systems Manager créé par Quick Setup installe l' CloudWatch agent et le configure avec la configuration par défaut de l' CloudWatch agent. La CloudWatch configuration par défaut s'aligne sur l'ensemble de mesures de base prédéfini. Vous devez remplacer l'étape de configuration par défaut et ajouter des étapes pour télécharger vos fichiers de CloudWatch configuration depuis votre compartiment de CloudWatch configuration S3.

Passez en revue le document InstallAndManageCloudWatchDocument.yaml mis à jour terminé et comparez-le au document créé par Quick Setup. Le document créé par votre installation rapide peut être différent, alors assurez-vous d'avoir effectué les ajustements nécessaires. Modifiez votre document existant pour inclure les étapes et modifications nécessaires.

Utiliser CloudFormation au lieu de Quick Setup

Au lieu d'utiliser Quick Setup, vous pouvez CloudFormation configurer Systems Manager. Cette approche vous permet de personnaliser la configuration de votre Systems Manager en fonction de vos besoins spécifiques. Cette approche permet également d'éviter les mises à jour manuelles des ressources configurées de Systems Manager créées par Quick Setup pour prendre en charge les CloudWatch configurations personnalisées.

La fonctionnalité Quick Setup utilise CloudFormation et crée également un ensemble de CloudFormation piles pour déployer et configurer les ressources de Systems Manager en fonction de vos choix. Avant de pouvoir utiliser des ensembles de CloudFormation piles, vous devez créer les rôles IAM utilisés pour CloudFormation StackSets prendre en charge les déploiements sur plusieurs comptes ou régions. La configuration rapide crée les rôles nécessaires pour prendre en charge les déploiements multirégionaux ou multicomptes. CloudFormation StackSets Vous devez remplir les conditions requises pour CloudFormation StackSets configurer et déployer les ressources de Systems Manager dans plusieurs régions ou sur plusieurs comptes à partir d'un seul compte et d'une seule région. Pour plus d'informations à ce sujet, consultez la section Conditions requises pour les opérations de stack set dans la CloudFormation documentation.

Consultez le CloudFormation modèle AWS- QuickSetup - SSMHost Mgmt.yaml pour une configuration rapide personnalisée.

Vous devez passer en revue les ressources et les fonctionnalités du CloudFormation modèle et apporter les modifications nécessaires en fonction de vos besoins. Vous devez contrôler la version du CloudFormation modèle que vous utilisez et tester progressivement les modifications pour confirmer le résultat requis. En outre, vous devez effectuer des examens de la sécurité du cloud afin de déterminer si des ajustements de politique sont nécessaires en fonction des exigences de votre organisation.

Vous devez déployer la CloudFormation pile dans un seul compte de test et une seule région, et effectuer tous les tests nécessaires pour personnaliser et confirmer le résultat souhaité. Vous pouvez ensuite étendre votre déploiement à plusieurs régions dans un seul compte, puis à plusieurs comptes et à plusieurs régions.

Configuration rapide personnalisée dans un seul compte et une seule région avec une CloudFormation pile

Si vous n'utilisez qu'un seul compte et une seule région, vous pouvez déployer l'exemple complet sous forme de CloudFormation pile au lieu d'un ensemble de CloudFormation piles. Toutefois, dans la mesure du possible, nous vous recommandons d'utiliser l'approche multi-comptes et multi-régions, même si vous n'utilisez qu'un seul compte et une seule région. L'utilisation CloudFormation StackSets facilite l'extension à d'autres comptes et régions à l'avenir.

Suivez les étapes suivantes pour déployer le CloudFormation modèle AWS- QuickSetup - SSMHost Mgmt.yaml sous forme de CloudFormation pile dans un seul compte et : Région AWS

1. Téléchargez le modèle et enregistrez-le dans votre système de contrôle de version préféré (par exemple, GitHub).
2. Personnalisez les valeurs des CloudFormation paramètres par défaut en fonction des besoins de votre organisation.
3. Personnalisez les plannings des associations State Manager.
4. Personnalisez le document Systems Manager avec l'ID `InstallAndManageCloudWatchDocument` logique. Vérifiez que les préfixes du compartiment S3 correspondent aux préfixes du compartiment S3 contenant votre CloudWatch configuration.
5. Récupérez et enregistrez le nom de ressource Amazon (ARN) du compartiment S3 contenant vos CloudWatch configurations. Pour plus d'informations à ce sujet, consultez la Gestion des CloudWatch configurations section de ce guide. Un exemple de CloudFormation modèle cloudwatch-config-sà 3 compartiments .yaml est disponible. Il inclut une politique de compartiment pour fournir un accès en lecture aux comptes. AWS Organizations

6. Déployez le CloudFormation modèle de configuration rapide personnalisé sur le même compte que votre compartiment S3 :
   - Pour le `CloudWatchConfigBucketARN` paramètre, entrez l'ARN du compartiment S3.
   - Ajustez les options des paramètres en fonction des fonctionnalités que vous souhaitez activer pour Systems Manager.

7. Déployez une EC2 instance de test avec ou sans rôle IAM pour vérifier que l' EC2instance fonctionne avec CloudWatch.

- Appliquez l'association `AttachIAMToInstance` State Manager. Il s'agit d'un runbook de Systems Manager configuré pour s'exécuter selon un calendrier. Les associations State Manager qui utilisent des runbooks ne sont pas automatiquement appliquées aux nouvelles EC2 instances et peuvent être configurées pour s'exécuter de manière planifiée. Pour plus d'informations, consultez la section Exécution d'automatismes avec des déclencheurs à l'aide de State Manager dans la documentation de Systems Manager.
- Vérifiez que le rôle IAM requis est attaché à l' EC2 instance.
- Vérifiez que l'agent Systems Manager fonctionne correctement en vérifiant que l' EC2instance est visible dans Systems Manager.
- Vérifiez que l' CloudWatch agent fonctionne correctement en consultant CloudWatch les journaux et les métriques en fonction des CloudWatch configurations de votre compartiment S3.

Configuration rapide personnalisée dans plusieurs régions et plusieurs comptes avec CloudFormation StackSets

Si vous utilisez plusieurs comptes et régions, vous pouvez déployer le CloudFormation modèle AWS-QuickSetup - SSMHost Mgmt.yaml sous forme de stack set. Vous devez remplir les CloudFormation StackSetprérequis avant d'utiliser des ensembles de piles. Les exigences varient selon que vous déployez des ensembles de piles avec des autorisations autogérées ou gérées par des services.

Nous vous recommandons de déployer des ensembles de piles dotés d'autorisations gérées par les services afin que les nouveaux comptes bénéficient automatiquement de la configuration rapide personnalisée. Vous devez déployer un ensemble de piles gérées par des services à partir du compte de AWS Organizations gestion ou du compte d'administrateur délégué. Vous devez déployer le stack set à partir d'un compte centralisé utilisé pour l'automatisation doté de privilèges d'administrateur délégués, plutôt que du compte AWS Organizations de gestion. Nous

vous recommandons également de tester le déploiement de votre stack set en ciblant une unité organisationnelle (UO) de test dotée d'un seul compte ou d'un petit nombre de comptes dans une région.

1. Effectuez les étapes 1 à 5 de la Configuration rapide personnalisée dans un seul compte et une seule région avec une CloudFormation pile section de ce guide.
2. Connectez-vous au AWS Management Console, ouvrez la CloudFormation console et choisissez Create StackSet :
   - Choisissez Le modèle est prêt et téléchargez un fichier modèle. Téléchargez le CloudFormation modèle que vous avez personnalisé selon vos besoins.
   - Spécifiez les détails de l'ensemble de piles :
     - Entrez le nom d'un ensemble de piles, par exemple,`StackSet-SSM-QuickSetup`.
     - Ajustez les options des paramètres en fonction des fonctionnalités que vous souhaitez activer pour Systems Manager.
     - Pour le `CloudWatchConfigBucketARN` paramètre, entrez l'ARN du compartiment S3 de votre CloudWatch configuration.
     - Spécifiez les options de l'ensemble de piles, choisissez si vous souhaitez utiliser des autorisations gérées par le service avec AWS Organizations ou des autorisations autogérées.
       - Si vous choisissez des autorisations autogérées, entrez les détails du rôle AWSCloudFormationStackSetAdministrationRoleet AWSCloudFormationStackSetExecutionRoleIAM. Le rôle d'administrateur doit exister dans le compte et le rôle d'exécution doit exister dans chaque compte cible
     - Pour les autorisations gérées par les services avec AWS Organizations, nous vous recommandons de déployer d'abord sur une unité d'organisation de test plutôt que sur l'ensemble de l'organisation.
       - Choisissez si vous souhaitez activer les déploiements automatiques. Nous vous recommandons de choisir Activé. Pour le comportement de suppression de comptes, le paramètre recommandé est Supprimer les piles.
     - Pour les autorisations autogérées, entrez le AWS compte IDs des comptes que vous souhaitez configurer. Vous devez répéter ce processus pour chaque nouveau compte si vous utilisez des autorisations autogérées.
     - Entrez les régions dans lesquelles vous allez utiliser CloudWatch et Systems Manager.
     - Vérifiez que le déploiement est réussi en consultant l'état de l'ensemble de piles dans l'onglet Opérations et instances de pile.

- Vérifiez que Systems Manager fonctionne correctement dans les comptes déployés en suivant l'étape 7 de la Configuration rapide personnalisée dans un seul compte et une seule région avec une CloudFormation pile section de ce guide. CloudWatch

Considérations relatives à la configuration des serveurs sur site

L' CloudWatch agent pour les serveurs sur site VMs est installé et configuré en utilisant une approche similaire à celle utilisée pour les EC2 instances. Toutefois, le tableau suivant fournit des éléments à prendre en compte lors de l'installation et de la configuration de l' CloudWatch agent sur des serveurs locaux et VMs.

Dirigez l' CloudWatch agent vers les mêmes informations d'identification temporaires que celles utilisées pour Systems Manager.	Lorsque vous configurez Systems Manager dans un environnement hybride incluant des serveurs sur site, vous pouvez activer Systems Manager avec un rôle IAM. Vous devez utiliser le rôle créé pour vos EC2 instances qui inclut les `AmazonSSMManagedInstanceCore` politiques `CloudWatchAgentServerPolicy` et. Cela permet à l'agent Systems Manager de récupérer et d'écrire des informations d'identification temporaires dans un fichier d'informations d'identification local. Vous pouvez faire pointer la configuration de votre CloudWatch agent vers le même fichier. Vous pouvez utiliser le processus de configuration des serveurs sur site qui utilisent l'agent Systems Manager et l' CloudWatch agent unifié pour n'utiliser que des informations d'identification temporaires dans le AWS Knowledge Center. Vous pouvez également automatiser ce processus en définissant une association distincte entre le runbook Systems Manager Automation et le State Manager, et en ciblant

	vos instances locales à l'aide de balises. Lorsque vous créez une activation de Systems Manager pour vos instances locales, vous devez inclure une balise identifiant les instances en tant qu'instances sur site.
Envisagez d'utiliser des comptes et des régions dotés d'un VPN ou Direct Connect d'un accès et AWS PrivateLink.	Vous pouvez utiliser AWS Direct Connect ou AWS Virtual Private Network (Site-to-Site VPN) pour établir des connexions privées entre les réseaux locaux et votre cloud privé virtuel (VPC). AWS PrivateLinkétablit une connexion privée aux CloudWatch journaux avec un point de terminaison VPC d'interface. Cette approche est utile si vous avez des restrictions qui empêchent l'envoi de données via l'Interne t public à un point de terminaison de service public.
Toutes les métriques doivent être incluses dans le fichier CloudWatch de configuration.	Amazon EC2 inclut des métriques standard (par exemple, l'utilisation du processeur) mais ces métriques doivent être définies pour les instances sur site. Vous pouvez utiliser un fichier de configuration de plate-forme distinct pour définir ces mesures pour les serveurs locaux, puis ajouter la configuration à la configuration CloudWatch des métriques standard de la plate-forme.

Considérations relatives aux instances éphémères EC2

EC2 les instances sont temporaires ou éphémères si elles sont mises en service par Amazon EC2 Auto Scaling, Amazon EMR, Amazon EC2 Spot Instances ou. AWS Batch EC2 Les instances éphémères peuvent générer un très grand nombre de CloudWatch flux dans un groupe de journaux commun sans informations supplémentaires sur leur origine d'exécution.

Si vous utilisez des EC2 instances éphémères, pensez à ajouter des informations contextuelles dynamiques supplémentaires dans les noms des groupes de journaux et des flux de journaux. Par

exemple, vous pouvez inclure l'ID de demande d'instance Spot, le nom du cluster Amazon EMR ou le nom du groupe Amazon EC2 Auto Scaling. Ces informations peuvent varier selon les EC2 instances récemment lancées et vous devrez peut-être les récupérer et les configurer au moment de l'exécution. Vous pouvez le faire en écrivant un fichier de configuration de CloudWatch l'agent au démarrage et en redémarrant l'agent pour inclure le fichier de configuration mis à jour. Cela permet de fournir des journaux et des métriques à CloudWatch l'aide d'informations d'exécution dynamiques.

Vous devez également vous assurer que vos statistiques et vos journaux sont envoyés par l' CloudWatch agent avant que vos EC2 instances éphémères ne soient résiliées. L' CloudWatch agent inclut un `flush_interval` paramètre qui peut être configuré pour définir l'intervalle de temps nécessaire au vidage des journaux et des tampons métriques. Vous pouvez réduire cette valeur en fonction de votre charge de travail, arrêter l' CloudWatch agent et forcer les tampons à se vider avant que l' EC2 instance ne soit mise hors service.

Utilisation d'une solution automatisée pour déployer l' CloudWatch agent

Si vous utilisez une solution d'automatisation (par exemple, Ansible ou Chef), vous pouvez en tirer parti pour installer et mettre à jour automatiquement l' CloudWatch agent. Si vous utilisez cette approche, vous devez prendre en compte les considérations suivantes :

- Vérifiez que l'automatisation couvre les versions du système OSs d'exploitation que vous prenez en charge. Si le script d'automatisation ne prend pas en charge tous ceux de votre organisation OSs, vous devez définir des solutions alternatives pour ceux qui ne le sont pas OSs.
- Vérifiez que la solution d'automatisation vérifie régulièrement les mises à jour et les mises à niveau des CloudWatch agents. Votre solution d'automatisation doit vérifier régulièrement les mises à jour de l' CloudWatch agent ou le désinstaller et le réinstaller régulièrement. Vous pouvez utiliser un planificateur ou une fonctionnalité de solution d'automatisation pour vérifier et mettre à jour régulièrement l'agent.
- Vérifiez que vous pouvez confirmer la conformité de l'installation et de la configuration de l'agent. Votre solution d'automatisation doit vous permettre de déterminer quand l'agent n'est pas installé sur un système ou quand l'agent ne fonctionne pas. Vous pouvez implémenter une notification ou une alarme dans votre solution d'automatisation afin de suivre les installations et les configurations défaillantes.

Déploiement de l' CloudWatch agent lors du provisionnement de l'instance avec le script de données utilisateur

Vous pouvez utiliser cette approche si vous n'avez pas l'intention d'utiliser Systems Manager et que vous souhaitez l'utiliser de manière sélective CloudWatch pour vos EC2 instances. Généralement, cette approche est utilisée une fois ou lorsqu'une configuration spécialisée est requise. AWS fournit des liens directs vers l' CloudWatch agent qui peuvent être téléchargés dans vos scripts de démarrage ou de données utilisateur. Les packages d'installation de l'agent peuvent être exécutés silencieusement sans intervention de l'utilisateur, ce qui signifie que vous pouvez les utiliser dans des déploiements automatisés. Si vous utilisez cette approche, vous devez prendre en compte les considérations suivantes :

- Risque accru que les utilisateurs n'installent pas l'agent ou ne configurent pas les métriques standard. Les utilisateurs peuvent provisionner des instances sans inclure les étapes nécessaires à l'installation de l' CloudWatch agent. Ils peuvent également mal configurer l'agent, ce qui peut entraîner des incohérences dans la journalisation et la surveillance.
- Les scripts d'installation doivent être spécifiques au système d'exploitation et adaptés aux différentes versions du système d'exploitation. Vous avez besoin de scripts distincts si vous comptez utiliser à la fois Windows et Linux. Le script Linux doit également comporter des étapes d'installation différentes en fonction de la distribution.
- Vous devez régulièrement mettre à jour l' CloudWatch agent avec les nouvelles versions lorsqu'elles sont disponibles. Cela peut être automatisé si vous utilisez Systems Manager avec State Manager, mais vous pouvez également configurer le script de données utilisateur pour qu'il soit réexécuté au démarrage de l'instance. L' CloudWatch agent est ensuite mis à jour et réinstallé à chaque redémarrage.
- Vous devez automatiser la récupération et l'application des CloudWatch configurations standard. Cela peut être automatisé si vous utilisez Systems Manager avec State Manager, mais vous pouvez également configurer un script de données utilisateur pour récupérer les fichiers de configuration au démarrage et redémarrer l' CloudWatch agent.

Inclure l' CloudWatch agent dans votre AMIs

L'avantage de cette approche est que vous n'avez pas à attendre que l' CloudWatch agent soit installé et configuré, et que vous pouvez immédiatement commencer à enregistrer et à surveiller. Cela vous permet de mieux surveiller le provisionnement de vos instances et les étapes de

démarrage au cas où les instances ne démarreraient pas. Cette approche est également appropriée si vous ne prévoyez pas d'utiliser l'agent Systems Manager. Si vous utilisez cette approche, vous devez prendre en compte les considérations suivantes :

- Un processus de mise à jour doit exister car il est AMIs possible qu'il n'inclue pas la version la plus récente de CloudWatch l'agent. L' CloudWatch agent installé dans une AMI n'est à jour que jusqu'à la dernière création de l'AMI. Vous devez inclure une méthode supplémentaire pour mettre à jour l'agent régulièrement et lors du provisionnement de l' EC2 instance. Si vous utilisez Systems Manager, vous pouvez utiliser la Installation de l' CloudWatch agent à l'aide de Systems Manager Distributor et State Manager solution fournie dans ce guide à cet effet. Si vous n'utilisez pas Systems Manager, vous pouvez utiliser un script de données utilisateur pour mettre à jour l'agent au démarrage et au redémarrage de l'instance.
- Le fichier de configuration de votre CloudWatch agent doit être récupéré au démarrage de l'instance. Si vous n'utilisez pas Systems Manager, vous pouvez configurer un script de données utilisateur pour récupérer les fichiers de configuration au démarrage, puis redémarrer l' CloudWatch agent.
- L' CloudWatch agent doit être redémarré après la mise à jour CloudWatch de votre configuration.
- AWS les informations d'identification ne doivent pas être enregistrées dans l'AMI. Assurez-vous qu'aucune information AWS d'identification locale n'est stockée dans l'AMI. Si vous utilisez Amazon EC2, vous pouvez appliquer le rôle IAM nécessaire à votre instance et éviter les informations d'identification locales. Si vous utilisez des instances sur site, vous devez automatiser ou mettre à jour manuellement les informations d'identification de l'instance avant de démarrer l' CloudWatch agent.

Journalisation et surveillance sur Amazon ECS

Amazon Elastic Container Service (Amazon ECS) propose deux types de lancement pour exécuter des conteneurs et qui déterminent le type d'infrastructure hébergeant les tâches et les services ; ces types de lancement sont AWS Fargate et Amazon. EC2 Les deux types de lancement s'intègrent CloudWatch , mais les configurations et le support varient.

Les sections suivantes vous aident à comprendre comment les utiliser CloudWatch pour la journalisation et la surveillance sur Amazon ECS.

Rubriques

- Configuration CloudWatch avec un type de EC2 lancement
- Journaux de conteneurs Amazon ECS pour les types de lancement de EC2 Fargate et les types de lancement
- Utilisation du routage personnalisé des journaux avec FireLens pour Amazon ECS
- Métriques pour Amazon ECS

Configuration CloudWatch avec un type de EC2 lancement

Avec un type de EC2 lancement, vous mettez en service un cluster Amazon ECS d' EC2 instances qui utilisent l' CloudWatchagent pour la journalisation et la surveillance. Une AMI optimisée pour Amazon ECS est préinstallée avec l'agent de conteneur Amazon ECS et fournit des CloudWatch métriques pour le cluster Amazon ECS.

Ces mesures par défaut sont incluses dans le coût d'Amazon ECS, mais la configuration par défaut d'Amazon ECS ne surveille pas les fichiers journaux ni les mesures supplémentaires (par exemple, l'espace disque disponible). Vous pouvez utiliser le AWS Management Console pour approvisionner un cluster Amazon ECS avec le type de EC2 lancement, cela crée une CloudFormation pile qui déploie un Amazon EC2 Auto Scaling groupe avec une configuration de lancement. Toutefois, cette approche signifie que vous ne pouvez pas choisir une AMI personnalisée ou personnaliser la configuration de lancement avec des paramètres différents ou des scripts de démarrage supplémentaires.

Pour surveiller des journaux et des métriques supplémentaires, vous devez installer l' CloudWatch agent sur vos instances de conteneur Amazon ECS. Vous pouvez utiliser l'approche d'installation

pour les EC2 instances décrite dans la Installation de l' CloudWatch agent à l'aide de Systems Manager Distributor et State Manager section de ce guide. Cependant, l'AMI Amazon ECS n'inclut pas l'agent Systems Manager requis. Vous devez utiliser une configuration de lancement personnalisée avec un script de données utilisateur qui installe l'agent Systems Manager lorsque vous créez votre cluster Amazon ECS. Cela permet à vos instances de conteneur de s'enregistrer auprès de Systems Manager et d'appliquer les associations State Manager pour installer, configurer et mettre à jour l' CloudWatch agent. Lorsque State Manager exécute et met à jour la configuration de votre CloudWatch agent, il applique également votre CloudWatch configuration standardisée au niveau du système pour Amazon. EC2 Vous pouvez également stocker des CloudWatch configurations standardisées pour Amazon ECS dans le compartiment S3 correspondant à votre CloudWatch configuration et les appliquer automatiquement avec State Manager.

Vous devez vous assurer que le rôle ou le profil d'instance IAM appliqué à vos instances de conteneur Amazon ECS inclut les exigences `CloudWatchAgentServerPolicy` et `AmazonSSMManagedInstanceCore` les politiques. Vous pouvez utiliser le modèle ecs_cluster_with_cloudwatch_linux.yaml pour CloudFormation provisionner des clusters Amazon ECS basés sur Linux. Ce modèle crée un cluster Amazon ECS avec une configuration de lancement personnalisée qui installe Systems Manager et déploie une CloudWatch configuration personnalisée pour surveiller les fichiers journaux spécifiques à Amazon ECS.

Vous devez capturer les journaux suivants pour vos instances de conteneur Amazon ECS, ainsi que vos journaux d' EC2 instance standard :

- Résultat de démarrage de l'agent Amazon ECS : `/var/log/ecs/ecs-init.log`
- Sortie de l'agent Amazon ECS : `/var/log/ecs/ecs-agent.log`
- Journal des demandes du fournisseur d'informations d'identification IAM — `/var/log/ecs/audit.log`

Pour plus d'informations sur le niveau de sortie, le formatage et les options de configuration supplémentaires, consultez les emplacements des fichiers journaux Amazon ECS dans la documentation Amazon ECS.

> **Important**
>
> L'installation ou la configuration de l'agent n'est pas requise pour le type de lancement Fargate, car vous n'exécutez ni EC2 ne gérez d'instances de conteneur.

Les instances de conteneur Amazon ECS doivent utiliser le dernier agent de conteneur optimisé AMIs et optimisé pour Amazon ECS. AWS stocke les paramètres publics du magasin de paramètres de Systems Manager avec les informations de l'AMI optimisées pour Amazon ECS, y compris l'ID de l'AMI. Vous pouvez récupérer l'AMI optimisée la plus récente depuis le magasin de paramètres en utilisant le format de paramètres du magasin de paramètres pour Amazon ECS optimisé AMIs. Vous pouvez faire référence au paramètre public Parameter Store qui fait référence à l'AMI la plus récente ou à une version d'AMI spécifique dans vos CloudFormation modèles.

AWS fournit les mêmes paramètres de magasin de paramètres dans chaque région prise en charge. Cela signifie que les CloudFormation modèles faisant référence à ces paramètres peuvent être réutilisés entre les régions et les comptes sans que l'AMI ne soit mise à jour. Vous pouvez contrôler le déploiement de la nouvelle version d'Amazon ECS AMIs dans votre organisation en vous référant à une version spécifique, ce qui vous permet d'empêcher l'utilisation d'une nouvelle AMI optimisée pour Amazon ECS tant que vous ne l'avez pas testée.

Journaux de conteneurs Amazon ECS pour les types de lancement de EC2 Fargate et les types de lancement

Amazon ECS utilise une définition de tâche pour déployer et gérer des conteneurs sous forme de tâches et de services. Vous configurez les conteneurs que vous souhaitez lancer dans votre cluster Amazon ECS dans le cadre d'une définition de tâche. La journalisation est configurée avec un pilote de journal au niveau du conteneur. Plusieurs options de pilote de journal fournissent à vos conteneurs différents systèmes de journalisation (par exemple `awslogs`,`fluentd`,`gelf`,`json-file`,`journald`,`logentries`, `splunk`,`syslog`, ou`awsfirelens`) selon que vous utilisez le type de lancement EC2 ou Fargate. Le type de lancement Fargate fournit un sous-ensemble des options `awslogs` de pilote de journal suivantes :, et. `splunk` `awsfirelens` AWS fournit le pilote de `awslogs` journal pour capturer et transmettre la sortie du conteneur à CloudWatch Logs. Les paramètres du pilote de journal vous permettent de personnaliser le groupe de journaux, la région et le préfixe du flux de journaux, ainsi que de nombreuses autres options.

Le nom par défaut pour les groupes de journaux et l'option utilisée par l'option Configuration automatique CloudWatch des journaux sur le AWS Management Console sont`/ecs/<task_name>`. Le nom du flux de journal utilisé par Amazon ECS est au `<awslogs-stream-prefix>/<container_name>/<task_id>` format suivant. Nous vous recommandons d'utiliser un nom de groupe qui regroupe vos journaux en fonction des besoins de votre organisation. Dans le tableau suivant, les `image_name` et `image_tag` sont inclus dans le nom du flux de log.

Nom du groupe de journaux	`/<Business unit>/<Project or application name>/<Environment>/<Cluster name>/<Task name>`
Préfixe du nom du flux de log	`/<image_name>/<image_tag>`

Ces informations sont également disponibles dans la définition de la tâche. Cependant, les tâches sont régulièrement mises à jour avec de nouvelles révisions, ce qui signifie que la définition de tâche peut avoir utilisé une version différente `image_name` de `image_tag` celle que la définition de tâche utilise actuellement. Pour plus d'informations et pour des suggestions de dénomination, consultez la Planification de votre CloudWatch déploiement section de ce guide.

Si vous utilisez un CI/CD) pipeline or automated process, you can create a new task definition revision for your application with each new Docker image build. For example, you can include the Docker image name, image tag, GitHub revision, or other important information in your task definition revision and logging configuration as a part of your CI/CD processus (processus) d'intégration et de livraison continues.

Utilisation du routage personnalisé des journaux avec FireLens pour Amazon ECS

FireLens pour Amazon ECS vous permet d'acheminer les journaux vers Fluentd ou Fluent Bit afin que vous puissiez envoyer directement les journaux des conteneurs vers les AWS services et les destinations du réseau de AWS partenaires (APN) et prendre en charge l'expédition des journaux vers Logs. CloudWatch

AWS fournit une image Docker pour Fluent Bit avec des plugins préinstallés pour Amazon Kinesis Data Streams, Amazon Data Firehose et Logs. CloudWatch Vous pouvez utiliser le pilote de FireLens journal au lieu du pilote de `awslogs` journal pour une personnalisation et un contrôle accrus des journaux envoyés à CloudWatch Logs.

Par exemple, vous pouvez utiliser le pilote de FireLens journal pour contrôler le format de sortie du journal. Cela signifie que les CloudWatch journaux d'un conteneur Amazon ECS sont automatiquement formatés sous forme d'objets JSON et incluent des propriétés au format JSON pour`ecs_cluster`,,, `ecs_task_arn`ecs_task_definition, `container_id` et.

`container_name` `ec2_instance_id` L'hôte fluide est exposé à votre conteneur via les variables d'`FLUENT_PORT`environnement `FLUENT_HOST` et lorsque vous spécifiez le `awsfirelens` pilote. Cela signifie que vous pouvez vous connecter directement au routeur de journalisation à partir de votre code en utilisant les bibliothèques Fluent Logger. Par exemple, votre application peut inclure la `fluent-logger-python` bibliothèque permettant de se connecter à Fluent Bit en utilisant les valeurs disponibles dans les variables d'environnement.

Si vous choisissez de l'utiliser FireLens pour Amazon ECS, vous pouvez configurer les mêmes paramètres que le pilote de `awslogs` journal et utiliser d'autres paramètres également. Par exemple, vous pouvez utiliser la définition de tâche Amazon ECS ecs-task-nginx-firelense.json qui lance un serveur NGINX configuré pour être utilisé FireLens pour la connexion à. CloudWatch Il lance également un conteneur FireLens Fluent Bit en tant que sidecar pour l'exploitation forestière.

Métriques pour Amazon ECS

Amazon ECS fournit des CloudWatch métriques standard (par exemple, l'utilisation du processeur et de la mémoire) pour les types de lancement EC2 et Fargate au niveau du cluster et du service avec l'agent de conteneur Amazon ECS. Vous pouvez également capturer des métriques pour vos services, tâches et conteneurs à l'aide de CloudWatch Container Insights, ou capturer vos propres métriques de conteneur personnalisées à l'aide du format de métrique intégré.

Container Insights est une CloudWatch fonctionnalité qui fournit des mesures telles que l'utilisation du processeur, l'utilisation de la mémoire, le trafic réseau et le stockage au niveau du cluster, de l'instance de conteneur, du service et des tâches. Container Insights crée également des tableaux de bord automatiques qui vous aident à analyser les services et les tâches, et à voir l'utilisation moyenne de la mémoire ou du processeur au niveau du conteneur. Container Insights publie des métriques personnalisées dans l'espace de noms `ECS/ContainerInsights` personnalisé que vous pouvez utiliser pour les graphiques, les alarmes et les tableaux de bord.

Vous pouvez activer les métriques Container Insight en activant Container Insights pour chaque cluster Amazon ECS individuel. Si vous souhaitez également consulter les métriques au niveau de l'instance de conteneur, vous pouvez lancer l' CloudWatch agent en tant que conteneur de démons sur votre cluster Amazon ECS. Vous pouvez utiliser le CloudFormation modèle cwagent-ecs-instance-metric-cfn.yaml pour déployer l'agent en CloudWatch tant que service Amazon ECS. Il est important de noter que cet exemple suppose que vous avez créé une configuration d' CloudWatchagent personnalisée appropriée et que vous l'avez stockée dans Parameter Store avec la clé`ecs-cwagent-daemon-service`.

L'CloudWatchagent déployé en tant que conteneur de démons pour CloudWatch Container Insights inclut des métriques supplémentaires relatives au disque, à la mémoire et au processeur, telles que `instance_cpu_reserved_capacity` et `instance_memory_reserved_capacity` avec les `InstanceId` dimensions `ClusterNameContainerInstanceId`,. Les métriques au niveau de l'instance de conteneur sont mises en œuvre par Container Insights en utilisant le format de métrique CloudWatch intégré. Vous pouvez configurer des métriques supplémentaires au niveau du système pour vos instances de conteneur Amazon ECS en utilisant l'approche décrite dans la Configurer State Manager et Distributor pour le déploiement et la configuration des CloudWatch agents section de ce guide.

Création de métriques d'application personnalisées dans Amazon ECS

Vous pouvez créer des métriques personnalisées pour vos applications en utilisant le format de métrique CloudWatch intégré. Le pilote de `awslogs` journal peut interpréter les instructions de format métrique CloudWatch intégrées.

Dans l'exemple suivant, la variable d'`CW_CONFIG_CONTENT`environnement est définie sur le contenu du paramètre `cwagentconfig` Systems Manager Parameter Store. Vous pouvez exécuter l'agent avec cette configuration de base pour le configurer en tant que point de terminaison au format métrique intégré. Toutefois, ce n'est plus nécessaire.

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

Si vous déployez Amazon ECS sur plusieurs comptes et régions, vous pouvez utiliser un AWS Secrets Manager secret pour stocker votre CloudWatch configuration et configurer la politique secrète afin de la partager avec votre organisation. Vous pouvez utiliser l'option secrets dans votre définition de tâche pour définir la `CW_CONFIG_CONTENT` variable.

Vous pouvez utiliser les bibliothèques de formats métriques intégrés open source AWS fournies dans votre application et spécifier la variable d'`AWS_EMF_AGENT_ENDPOINT`environnement à connecter au conteneur annexe de votre CloudWatch agent agissant comme un point de terminaison

au format métrique intégré. Par exemple, vous pouvez utiliser l'exemple d'application Python ecs_cw_emf_example pour envoyer des métriques au format métrique intégré à CloudWatch un conteneur d'agent configuré comme point de terminaison au format métrique intégré.

Le plugin Fluent Bit pour CloudWatch peut également être utilisé pour envoyer des messages au format métrique intégré. Vous pouvez également utiliser l'exemple d'application Python ecs_firelense_emf_example pour envoyer des métriques au format métrique intégré à un conteneur annexe Firelens for Amazon ECS.

Si vous ne souhaitez pas utiliser le format de métrique intégré, vous pouvez créer et mettre à jour CloudWatch des métriques via l'AWS API ou le AWS SDK. Nous ne recommandons pas cette approche, sauf si vous avez un cas d'utilisation spécifique, car elle ajoute des frais de maintenance et de gestion à votre code.

Journalisation et surveillance dans Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) CloudWatch s'intègre aux journaux pour le plan de contrôle Kubernetes. Le plan de contrôle est fourni en tant que service géré par Amazon EKS et vous pouvez activer la journalisation sans installer d' CloudWatchagent. L' CloudWatch agent peut également être déployé pour capturer les journaux des nœuds et des conteneurs Amazon EKS. Fluent Bit et Fluentd sont également pris en charge pour envoyer les journaux de vos conteneurs à CloudWatch Logs.

CloudWatch Container Insights fournit une solution complète de surveillance des métriques pour Amazon EKS au niveau du cluster, du nœud, du pod, de la tâche et du service. Amazon EKS prend également en charge plusieurs options pour la capture des métriques avec Prometheus. Le plan de contrôle Amazon EKS fournit un point de terminaison de métriques qui expose les métriques au format Prometheus. Vous pouvez déployer Prometheus dans votre cluster Amazon EKS pour utiliser ces métriques.

Vous pouvez également configurer l' CloudWatch agent pour extraire les métriques Prometheus et CloudWatch créer des métriques, en plus de consommer d'autres points de terminaison Prometheus. La surveillance de Container Insights pour Prometheus permet également de découvrir et de capturer automatiquement les métriques Prometheus à partir de charges de travail et de systèmes conteneurisés pris en charge.

Vous pouvez installer et configurer l' CloudWatch agent sur vos nœuds Amazon EKS, de la même manière que l'approche utilisée pour Amazon EC2 avec Distributor and State Manager, afin d'aligner vos nœuds Amazon EKS sur les configurations standard de journalisation et de surveillance de votre système.

Journalisation pour Amazon EKS

La journalisation Kubernetes peut être divisée en journalisation du plan de contrôle, journalisation des nœuds et journalisation des applications. Le plan de contrôle Kubernetes est un ensemble de composants qui gèrent les clusters Kubernetes et produisent des journaux utilisés à des fins d'audit et de diagnostic. Avec Amazon EKS, vous pouvez activer les journaux pour les différents composants du plan de contrôle et les envoyer à CloudWatch.

Kubernetes exécute également des composants système tels que `kubelet` et `kube-proxy` sur chaque nœud Kubernetes qui exécute vos pods. Ces composants rédigent des journaux dans

chaque nœud et vous pouvez configurer CloudWatch Container Insights pour capturer ces journaux pour chaque nœud Amazon EKS.

Les conteneurs sont regroupés sous forme de pods au sein d'un cluster Kubernetes et sont planifiés pour s'exécuter sur vos nœuds Kubernetes. La plupart des applications conteneurisées écrivent en sortie standard et en erreur standard, et le moteur de conteneur redirige la sortie vers un pilote de journalisation. Dans Kubernetes, les journaux des conteneurs se trouvent dans le `/var/log/pods` répertoire d'un nœud. Vous pouvez configurer CloudWatch Container Insights pour capturer ces journaux pour chacun de vos pods Amazon EKS.

Journalisation de plan de contrôle d'Amazon EKS

Un cluster Amazon EKS consiste en un plan de contrôle à haute disponibilité à locataire unique pour votre cluster Kubernetes et les nœuds Amazon EKS qui exécutent vos conteneurs. Les nœuds du plan de contrôle s'exécutent dans un compte géré par AWS. Les nœuds du plan de contrôle du cluster Amazon EKS sont intégrés CloudWatch et vous pouvez activer la journalisation pour des composants spécifiques du plan de contrôle.

Des journaux sont fournis pour chaque instance de composant du plan de contrôle Kubernetes. AWS gère l'état de santé des nœuds de votre plan de contrôle et fournit un accord de niveau de service (SLA) pour le point de terminaison Kubernetes.

Journalisation des applications et des nœuds Amazon EKS

Nous vous recommandons d'utiliser CloudWatchContainer Insights pour capturer les journaux et les métriques pour Amazon EKS. Container Insights implémente des métriques au niveau du cluster, du nœud et du pod avec l' CloudWatch agent, et Fluent Bit ou Fluentd pour la capture des journaux. CloudWatch Container Insights fournit également des tableaux de bord automatiques avec des vues en couches de vos CloudWatch indicateurs capturés. Container Insights est déployé sous forme CloudWatch DaemonSet de Fluent Bit DaemonSet qui s'exécute sur chaque nœud Amazon EKS. Les nœuds Fargate ne sont pas pris en charge par Container Insights car ils sont gérés AWS par et ne sont pas pris en charge. DaemonSets La journalisation Fargate pour Amazon EKS est traitée séparément dans ce guide.

Le tableau suivant indique les CloudWatch groupes de journaux et les journaux capturés par la configuration de capture de journaux Fluentd ou Fluent Bit par défaut pour Amazon EKS.

`/aws/containerinsights/Cluster_Name/application`	Tous les fichiers journaux sont enregistrés `/var/log/containers` . Ce répertoire fournit des liens symboliques vers tous les journaux des conteneurs Kubernetes dans la structure du `/var/log/pods` répertoire. Cela capture les journaux du conteneur de votre application écrivant dans `stdout` ou `stderr`. Il inclut également des journaux pour les conteneurs du système Kubernetes tels que `aws-vpc-cni-init` , et `kube-proxy` . `coreDNS`
`/aws/containerinsights/Cluster_Name/host`	Journaux provenant de `/var/log/dmesg` `/var/log/secure` , et `/var/log/messages` .
`/aws/containerinsights/Cluster_Name/dataplane`	Les journaux dans `/var/log/journal` pour `kubelet.service` , `kubeproxy.service` et `docker.service` .

Si vous ne souhaitez pas utiliser Container Insights avec Fluent Bit ou Fluentd pour la journalisation, vous pouvez capturer les journaux des nœuds et des conteneurs avec l' CloudWatch agent installé sur les nœuds Amazon EKS. Les nœuds Amazon EKS sont EC2 des instances, ce qui signifie que vous devez les inclure dans votre approche standard de journalisation au niveau du système pour Amazon. EC2 Si vous installez l' CloudWatch agent à l'aide de Distributor et State Manager, les nœuds Amazon EKS sont également inclus dans l'installation, la configuration et la mise à jour de l' CloudWatch agent.

Le tableau suivant indique les journaux spécifiques à Kubernetes que vous devez capturer si vous n'utilisez pas Container Insights avec Fluent Bit ou Fluentd pour la journalisation.

`/var/log/containers`	Ce répertoire fournit des liens symboliques vers tous les journaux des conteneurs Kubernetes dans la structure du `/var/log/pods`

	répertoire. Cela capture efficacement les journaux du conteneur de votre application qui écrivent dans `stdout` ou`stderr`. Cela inclut les journaux pour les conteneurs du système Kubernetes tels que`aws-vpc-cni-init` , et`kube-proxy` . `coreDNS` Important : cela n'est pas obligatoire si vous utilisez Container Insights.

`var/log/aws-routed-eni/ipamd.log`
 	
`/var/log/aws-routed-eni/plugin.log`
	Les journaux du démon L-IPAM se trouvent ici

Vous devez vous assurer que les nœuds Amazon EKS installent et configurent l' CloudWatch agent pour envoyer les journaux et mesures appropriés au niveau du système. Cependant, l'AMI optimisée pour Amazon EKS n'inclut pas l'agent Systems Manager. À l'aide de modèles de lancement, vous pouvez automatiser l'installation de l'agent Systems Manager et une CloudWatch configuration par défaut qui capture les journaux importants spécifiques à Amazon EKS à l'aide d'un script de démarrage implémenté via la section des données utilisateur. Les nœuds Amazon EKS sont déployés à l'aide d'un groupe Auto Scaling en tant que groupe de nœuds gérés ou en tant que nœuds autogérés.

Avec les groupes de nœuds gérés, vous fournissez un modèle de lancement qui inclut la section des données utilisateur pour automatiser l'installation et la CloudWatch configuration de l'agent Systems Manager. Vous pouvez personnaliser et utiliser le modèle amazon_eks_managed_node_group_launch_config.yaml pour créer un CloudFormation modèle de lancement qui installe l'agent Systems Manager, l'agent, et ajoute également une configuration de journalisation spécifique à Amazon EKS dans le répertoire de configuration. CloudWatch CloudWatch Ce modèle peut être utilisé pour mettre à jour votre modèle de lancement de groupes de nœuds gérés Amazon EKS selon une approche infrastructure-as-code (iAc). Chaque mise à jour du CloudFormation modèle fournit une nouvelle version du modèle de lancement. Vous pouvez ensuite mettre à jour le groupe de nœuds pour utiliser la nouvelle version du modèle et demander au processus de gestion du cycle de vie de mettre à jour vos nœuds sans interruption de service. Assurez-vous que le rôle IAM et le profil d'instance appliqués à votre

groupe de nœuds gérés incluent les politiques `AmazonSSMManagedInstanceCore` AWS gérées `CloudWatchAgentServerPolicy` et.

Avec les nœuds autogérés, vous provisionnez et gérez directement le cycle de vie et la stratégie de mise à jour de vos nœuds Amazon EKS. Les nœuds autogérés vous permettent d'exécuter des nœuds Windows sur votre cluster Amazon EKS et sur Bottlerocket, entre autres options. Vous pouvez utiliser CloudFormation pour déployer des nœuds autogérés dans vos clusters Amazon EKS, ce qui signifie que vous pouvez utiliser une approche iAc et une approche de modification gérée pour vos clusters Amazon EKS. AWS fournit le CloudFormation modèle amazon-eks-nodegroup.yaml que vous pouvez utiliser tel quel ou personnaliser. Le modèle fournit toutes les ressources requises pour les nœuds Amazon EKS d'un cluster (par exemple, un rôle IAM distinct, un groupe de sécurité, un groupe Amazon EC2 Auto Scaling et un modèle de lancement). Le CloudFormation modèle amazon-eks-nodegroup.yaml est une version mise à jour qui installe l'agent Systems Manager requis, l' CloudWatch agent, et ajoute également une configuration de journalisation spécifique à Amazon EKS dans le CloudWatch répertoire de configuration.

Journalisation pour Amazon EKS sur Fargate

Avec Amazon EKS sur Fargate, vous pouvez déployer des pods sans allouer ni gérer vos nœuds Kubernetes. Il n'est donc plus nécessaire de capturer des journaux au niveau du système pour vos nœuds Kubernetes. Pour capturer les journaux de vos pods Fargate, vous pouvez utiliser Fluent Bit pour les transférer directement vers. CloudWatch Cela vous permet d'acheminer automatiquement les journaux CloudWatch sans autre configuration ou vers un conteneur annexe pour vos pods Amazon EKS sur Fargate. Pour plus d'informations à ce sujet, consultez Fargate logging dans la documentation Amazon EKS et Fluent Bit pour Amazon EKS sur le blog. AWS Cette solution capture les flux `STDOUT` et `STDERR` input/output (E/S) de votre conteneur et les envoie CloudWatch via Fluent Bit, sur la base de la configuration Fluent Bit établie pour le cluster Amazon EKS sur Fargate.

Métriques pour Amazon EKS et Kubernetes

Kubernetes fournit une API de métriques qui vous permet d'accéder aux métriques d'utilisation des ressources (par exemple, l'utilisation du processeur et de la mémoire pour les nœuds et les pods), mais l'API fournit uniquement des point-in-time informations et non des métriques historiques. Le serveur de métriques Kubernetes est généralement utilisé pour les déploiements Amazon EKS et Kubernetes pour agréger les métriques, fournir des informations historiques à court terme sur les métriques et prendre en charge des fonctionnalités telles que Horizontal Pod Autoscaler.

Amazon EKS expose les métriques du plan de contrôle via le serveur d'API Kubernetes au format Prometheus et peut capturer et ingérer ces métriques. CloudWatch CloudWatch et Container Insights peut également être configuré pour fournir une capture, une analyse et des alarmes complètes de mesures pour vos nœuds et pods Amazon EKS.

Métriques du plan de contrôle Kubernetes

Kubernetes expose les métriques du plan de contrôle au format Prometheus en utilisant le point de terminaison de l'API HTTP. `/metrics` Vous devez installer Prometheus dans votre cluster Kubernetes pour représenter graphiquement et visualiser ces métriques dans un navigateur Web. Vous pouvez également ingérer les métriques exposées par le serveur d'API Kubernetes dans. CloudWatch

Métriques relatives aux nœuds et au système pour Kubernetes

Kubernetes fournit le module de serveur de mesures Prometheus que vous pouvez déployer et exécuter sur vos clusters Kubernetes pour obtenir des statistiques sur le processeur et la mémoire au niveau des clusters, des nœuds et des pods. Ces mesures sont utilisées avec le Horizontal Pod Autoscaler et le Vertical Pod Autoscaler. CloudWatch peut également fournir ces métriques.

Vous devez installer le serveur Kubernetes Metrics si vous utilisez le tableau de bord Kubernetes ou les autoscalers horizontaux et verticaux. Le tableau de bord Kubernetes vous permet de parcourir et de configurer votre cluster Kubernetes, vos nœuds, vos pods et la configuration associée, et de visualiser les métriques du processeur et de la mémoire à partir du serveur de métriques Kubernetes.

Les métriques fournies par le serveur de métriques Kubernetes ne peuvent pas être utilisées à des fins autres que le dimensionnement automatique (par exemple, pour la surveillance). Les métriques sont destinées à l' point-in-timeanalyse et non à l'analyse historique. Le tableau de bord Kubernetes déploie les métriques de stockage `dashboard-metrics-scraper` à partir du serveur de métriques Kubernetes pendant une courte période.

Container Insights utilise une version conteneurisée de l' CloudWatch agent qui s'exécute dans un Kubernetes DaemonSet pour découvrir tous les conteneurs actifs dans un cluster et fournir des métriques au niveau des nœuds. Il collecte des données de performance à chaque niveau de la pile de performances. Vous pouvez utiliser le Quick Start à partir de AWS Quick Starts ou configurer Container Insights séparément. Le Quick Start configure la surveillance des métriques avec l' CloudWatch agent et la journalisation avec Fluent Bit, de sorte que vous n'avez besoin de le déployer qu'une seule fois pour la journalisation et la surveillance.

Les nœuds Amazon EKS étant des EC2 instances, vous devez capturer les métriques au niveau des systèmes, en plus des métriques capturées par Container Insights, en utilisant les normes que vous avez définies pour Amazon. EC2 Vous pouvez utiliser la même approche décrite dans la Configurer State Manager et Distributor pour le déploiement et la configuration des CloudWatch agents section de ce guide pour installer et configurer l' CloudWatch agent pour vos clusters Amazon EKS. Vous pouvez mettre à jour votre fichier de CloudWatch configuration spécifique à Amazon EKS pour inclure des métriques ainsi que la configuration de journal spécifique à Amazon EKS.

L' CloudWatch agent compatible avec Prometheus peut automatiquement découvrir et extraire les métriques Prometheus à partir de charges de travail et de systèmes conteneurisés pris en charge. Il les ingère sous forme de CloudWatch journaux au format métrique intégré à des fins d'analyse avec CloudWatch Logs Insights et crée automatiquement CloudWatch des métriques.

> **Important**
>
> Vous devez déployer une version spécialisée de l' CloudWatch agent pour collecter les métriques Prometheus. Il s'agit d'un agent distinct de l' CloudWatch agent déployé pour Container Insights. Vous pouvez utiliser l'exemple d'application Java prometheus_jmx, qui inclut les fichiers de déploiement et de configuration pour le déploiement de l'agent CloudWatch et du pod Amazon EKS pour démontrer la découverte des métriques Prometheus. Pour plus d'informations, consultez la section Configurer un Java/JMX exemple de charge de travail sur Amazon EKS et Kubernetes dans la documentation. CloudWatch Vous pouvez également configurer l' CloudWatch agent pour qu'il capture les métriques d'autres cibles Prometheus exécutées dans votre cluster Amazon EKS.

Métriques d'application

Vous pouvez créer vos propres métriques personnalisées avec le format de métrique CloudWatch intégré. Pour ingérer des instructions au format métrique intégré, vous devez envoyer des entrées au format métrique intégré à un point de terminaison au format métrique intégré. L' CloudWatch agent peut être configuré en tant que conteneur annexe dans votre pod Amazon EKS. La configuration de l' CloudWatch agent est stockée sous forme de Kubernetes ConfigMap et lue par le conteneur annexe de votre CloudWatch agent pour démarrer le point de terminaison au format métrique intégré.

Vous pouvez également configurer votre application en tant que cible Prometheus et configurer CloudWatch l'agent, avec l'assistance de Prometheus, pour découvrir, extraire et intégrer vos indicateurs. CloudWatch Par exemple, vous pouvez utiliser l'exportateur JMX open source avec vos

applications Java pour exposer les haricots JMX destinés à la consommation de Prometheus par l'agent. CloudWatch

Si vous ne souhaitez pas utiliser le format de métrique intégré, vous pouvez également créer et mettre à jour des CloudWatch métriques à l'aide de l'AWS API ou du AWS SDK. Cependant, nous ne recommandons pas cette approche, car elle mélange la surveillance et la logique de l'application.

Métriques pour Amazon EKS sur Fargate

Fargate provisionne automatiquement les nœuds Amazon EKS pour exécuter vos pods Kubernetes. Vous n'avez donc pas besoin de surveiller et de collecter des métriques au niveau des nœuds. Cependant, vous devez surveiller les métriques des pods exécutés sur vos nœuds Amazon EKS sur Fargate. Container Insights n'est actuellement pas disponible pour Amazon EKS sur Fargate car il nécessite les fonctionnalités suivantes qui ne sont pas prises en charge actuellement :

- DaemonSets ne sont pas pris en charge actuellement. Container Insights est déployé en exécutant l' CloudWatch agent DaemonSet en tant que nœud de cluster.
- HostPath les volumes persistants ne sont pas pris en charge. Le conteneur CloudWatch d'agents utilise les volumes persistants HostPath comme condition préalable à la collecte des données métriques du conteneur.
- Fargate empêche les conteneurs privilégiés et l'accès aux informations de l'hôte.

Vous pouvez utiliser le routeur de log intégré auquel Fargate envoie des instructions au format métrique intégré. CloudWatch Le routeur de log utilise Fluent Bit, qui possède un CloudWatch plugin qui peut être configuré pour prendre en charge les instructions au format métrique intégrées.

Vous pouvez récupérer et capturer des métriques au niveau des pods pour vos nœuds Fargate en déployant le serveur Prometheus dans votre cluster Amazon EKS afin de recueillir des métriques à partir de vos nœuds Fargate. Prometheus nécessitant un stockage persistant, vous pouvez déployer Prometheus sur Fargate si vous utilisez Amazon Elastic File System (Amazon EFS) pour le stockage persistant. Vous pouvez également déployer Prometheus sur un nœud soutenu par Amazon EC2 . Pour plus d'informations, consultez la section Surveillance d'Amazon EKS sur AWS Fargate l'utilisation de Prometheus et Grafana sur le blog. AWS

Surveillance de Prometheus sur Amazon EKS

Amazon Managed Service for Prometheus fournit un service géré évolutif, sécurisé AWS et adapté à l'open source Prometheus. Vous pouvez utiliser le langage de requête Prometheus (ProMQL) pour surveiller les performances des charges de travail conteneurisées sans gérer l'infrastructure sous-jacente pour l'ingestion, le stockage et l'interrogation des métriques opérationnelles. Vous pouvez collecter des métriques Prometheus depuis Amazon EKS et Amazon ECS en AWS utilisant les serveurs Distro OpenTelemetry for (ADOT) ou Prometheus comme agents de collecte.

CloudWatch La surveillance de Container Insights pour Prometheus vous permet de configurer et d'utiliser CloudWatch l'agent pour découvrir les métriques Prometheus issues des charges de travail Amazon ECS, Amazon EKS et Kubernetes, et les ingérer sous forme de métriques. CloudWatch Cette solution est appropriée s'il s' CloudWatch agit de votre principale solution d'observabilité et de surveillance. Cependant, la liste suivante décrit les cas d'utilisation dans lesquels Amazon Managed Service for Prometheus offre plus de flexibilité pour ingérer, stocker et interroger les métriques Prometheus :

- Amazon Managed Service for Prometheus vous permet d'utiliser des serveurs Prometheus existants déployés dans Amazon EKS ou des serveurs Kubernetes autogérés et de les configurer pour écrire sur Amazon Managed Service for Prometheus au lieu d'un magasin de données configuré localement. Cela élimine le fardeau indifférencié lié à la gestion d'un magasin de données hautement disponible pour vos serveurs Prometheus et leur infrastructure. Amazon Managed Service for Prometheus est un choix approprié lorsque vous avez un déploiement Prometheus mature que vous souhaitez exploiter dans le cloud. AWS
- Grafana soutient directement Prometheus en tant que source de données pour la visualisation. Si vous souhaitez utiliser Grafana avec Prometheus plutôt que des CloudWatch tableaux de bord pour surveiller vos conteneurs, Amazon Managed Service for Prometheus peut répondre à vos besoins. Amazon Managed Service for Prometheus s'intègre à Amazon Managed Grafana pour fournir une solution de surveillance et de visualisation open source gérée.
- Prometheus vous permet d'analyser vos indicateurs opérationnels à l'aide de requêtes ProMQL. En revanche, l' CloudWatch agent ingère les métriques Prometheus au format CloudWatch métrique intégré dans les journaux, ce qui donne lieu à des métriques. CloudWatch Vous pouvez interroger les journaux au format métrique intégré à l'aide de CloudWatch Logs Insights.
- Si vous ne prévoyez pas de l'utiliser CloudWatch pour la surveillance et la capture de métriques, vous devez utiliser Amazon Managed Service for Prometheus avec votre serveur Prometheus et une solution de visualisation telle que Grafana. Vous devez configurer votre serveur Prometheus

pour extraire les métriques de vos cibles Prometheus et configurer le serveur pour écrire à distance dans votre espace de travail Amazon Managed Service for Prometheus. Si vous utilisez Amazon Managed Grafana, vous pouvez intégrer directement Amazon Managed Grafana à votre source de données Amazon Managed Service for Prometheus en utilisant le plugin inclus. Les données métriques étant stockées dans Amazon Managed Service for Prometheus, il n'y a aucune dépendance pour déployer CloudWatch l'agent ni aucune obligation d'y ingérer des données. CloudWatch L' CloudWatch agent est requis pour la surveillance de Container Insights pour Prometheus.

Vous pouvez également utiliser le collecteur ADOT pour extraire des données d'une application instrumentée par Prometheus et envoyer les métriques à Amazon Managed Service for Prometheus. Pour plus d'informations sur ADOT Collector, consultez la documentation de la AWS distribution. OpenTelemetry

Journalisation et statistiques pour AWS Lambda

Lambda élimine le besoin de gérer et de surveiller les serveurs pour vos charges de travail et fonctionne automatiquement avec CloudWatch les métriques et les CloudWatch journaux sans autre configuration ni instrumentation du code de votre application. Cette section vous aide à comprendre les caractéristiques de performance des systèmes utilisés par Lambda et l'influence de vos choix de configuration sur les performances. Il vous aide également à enregistrer et à surveiller vos fonctions Lambda afin d'optimiser les performances et de diagnostiquer les problèmes au niveau de l'application.

Journalisation des fonctions Lambda

Lambda diffuse automatiquement la sortie standard et les messages d'erreur standard d'une fonction Lambda vers CloudWatch Logs, sans avoir besoin de pilotes de journalisation. Lambda approvisionne également automatiquement les conteneurs qui exécutent votre fonction Lambda et les configure pour générer des messages de journal dans des flux de journal distincts.

Les appels ultérieurs de votre fonction Lambda peuvent réutiliser le même conteneur et le générer dans le même flux de journal. Lambda peut également provisionner un nouveau conteneur et envoyer l'invocation dans un nouveau flux de log.

Lambda crée automatiquement un groupe de journaux lorsque votre fonction Lambda est invoquée pour la première fois. Les fonctions Lambda peuvent avoir plusieurs versions et vous pouvez choisir la version que vous souhaitez exécuter. Tous les journaux des appels de la fonction Lambda sont stockés dans le même groupe de journaux. Le nom ne peut pas être modifié et est au `/aws/lambda/<YourLambdaFunctionName>` format. Un flux de journal distinct est créé dans le groupe de journaux pour chaque instance de fonction Lambda. Lambda dispose d'une convention de dénomination standard pour les flux de journaux qui utilise un `YYYY/MM/DD/[<FunctionVersion>]<InstanceId>` format. Le `InstanceId` est généré par AWS pour identifier l'instance de fonction Lambda.

Nous vous recommandons de formater vos messages de journal au format JSON, car vous pouvez les interroger plus facilement avec CloudWatch Logs Insights. Ils peuvent également être filtrés et exportés plus facilement. Vous pouvez utiliser une bibliothèque de journalisation pour simplifier ce processus ou créer vos propres fonctions de gestion des journaux. Nous vous recommandons d'utiliser une bibliothèque de journalisation pour faciliter le formatage et la classification des messages de journal. Par exemple, si votre fonction Lambda est écrite en Python, vous pouvez

utiliser le module de journalisation Python pour enregistrer les messages et contrôler le format de sortie. Lambda utilise nativement la bibliothèque de journalisation Python pour les fonctions Lambda écrites en Python, et vous pouvez récupérer et personnaliser l'enregistreur dans votre fonction Lambda. AWS Labs a créé la boîte à AWS Lambda outils pour développeurs Powertools for Python afin de faciliter l'enrichissement des messages de journal avec des données clés telles que les démarrages à froid. La boîte à outils est disponible pour Python, Java, Typescript et .NET.

Une autre bonne pratique consiste à définir le niveau de sortie du journal à l'aide d'une variable et à l'ajuster en fonction de l'environnement et de vos besoins. Le code de votre fonction Lambda, en plus des bibliothèques utilisées, peut générer une grande quantité de données de journal en fonction du niveau de sortie du journal. Cela peut avoir un impact sur vos coûts de journalisation et affecter les performances.

Lambda vous permet de définir des variables d'environnement pour l'environnement d'exécution de votre fonction Lambda sans mettre à jour votre code. Par exemple, vous pouvez créer une variable d'`LAMBDA_LOG_LEVEL`environnement qui définit le niveau de sortie du journal que vous pouvez récupérer à partir de votre code. L'exemple suivant tente de récupérer une variable d'`LAMBDA_LOG_LEVEL`environnement et d'utiliser la valeur pour définir le résultat de journalisation. Si la variable d'environnement n'est pas définie, elle prend par défaut le `INFO` niveau.

```
import logging
from os import getenv

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

Envoi de journaux vers d'autres destinations depuis CloudWatch

Vous pouvez envoyer des journaux vers d'autres destinations (par exemple, Amazon OpenSearch Service ou une fonction Lambda) en utilisant des filtres d'abonnement. Si vous n'utilisez pas Amazon OpenSearch Service, vous pouvez utiliser une fonction Lambda pour traiter les journaux et les envoyer au AWS service de votre choix à l'aide du. AWS SDKs

Vous pouvez également utiliser SDKs des destinations de journal en dehors du AWS Cloud dans votre fonction Lambda pour envoyer directement des instructions de journal à la destination de votre

choix. Si vous choisissez cette option, nous vous recommandons de prendre en compte l'impact de la latence, du temps de traitement supplémentaire, de la gestion des erreurs et des nouvelles tentatives, ainsi que du couplage de la logique opérationnelle à votre fonction Lambda.

Métriques de la fonction Lambda

Lambda vous permet d'exécuter votre code sans gérer ni dimensionner les serveurs, ce qui élimine pratiquement le fardeau des audits et des diagnostics au niveau du système. Cependant, il est toujours important de comprendre les indicateurs de performance et d'appel au niveau du système pour vos fonctions Lambda. Cela vous permet d'optimiser la configuration des ressources et d'améliorer les performances du code. La surveillance et la mesure efficaces des performances peuvent améliorer l'expérience utilisateur et réduire vos coûts en dimensionnant correctement vos fonctions Lambda. Généralement, les charges de travail exécutées sous forme de fonctions Lambda comportent également des métriques au niveau de l'application qui doivent être capturées et analysées. Lambda prend directement en charge le format de métrique intégré pour faciliter la capture des métriques au niveau de l'application. CloudWatch

Métriques au niveau du système

Lambda s'intègre automatiquement à CloudWatch Metrics et fournit un ensemble de métriques standard pour vos fonctions Lambda. Lambda fournit également un tableau de bord de surveillance distinct pour chaque fonction Lambda avec ces métriques. Les deux indicateurs importants que vous devez surveiller sont les erreurs et les erreurs d'invocation. Comprendre les différences entre les erreurs d'appel et les autres types d'erreur vous aide à diagnostiquer et à prendre en charge les déploiements Lambda.

Les erreurs d'invocation empêchent l'exécution de votre fonction Lambda. Ces erreurs se produisent avant l'exécution de votre code. Vous ne pouvez donc pas implémenter de gestion des erreurs dans votre code pour les identifier. Vous devez plutôt configurer des alarmes pour vos fonctions Lambda qui détectent ces erreurs et avertissent les responsables des opérations et des charges de travail. Ces erreurs sont souvent liées à une erreur de configuration ou d'autorisation et peuvent survenir à la suite d'une modification de votre configuration ou de vos autorisations. Les erreurs d'invocation peuvent déclencher une nouvelle tentative, ce qui entraîne plusieurs invocations de votre fonction.

Une fonction Lambda invoquée avec succès renvoie une réponse HTTP 200 même si une exception est déclenchée par la fonction. Vos fonctions Lambda doivent implémenter le traitement des erreurs et déclencher des exceptions afin que la `Errors` métrique capture et identifie les échecs d'exécution

de votre fonction Lambda. Vous devez renvoyer une réponse formatée à partir de vos appels de fonction Lambda qui inclut des informations permettant de déterminer si l'exécution a échoué complètement, partiellement ou s'est déroulée avec succès.

CloudWatch fournit des informations CloudWatch Lambda que vous pouvez activer pour une fonction Lambda individuelle. Lambda Insights collecte, agrège et résume les métriques au niveau du système (par exemple, le temps processeur, la mémoire, l'utilisation du disque et du réseau). Lambda Insights collecte, agrège et résume également les informations de diagnostic (par exemple, les démarrages à froid et les arrêts des opérateurs Lambda) pour vous aider à isoler et à résoudre rapidement les problèmes.

Lambda Insights utilise le format métrique intégré pour transmettre automatiquement des informations de performance au groupe de `/aws/lambda-insights/` journaux avec un préfixe de nom de flux de journal basé sur le nom de votre fonction Lambda. Ces événements du journal des performances créent CloudWatch des métriques qui constituent la base des CloudWatch tableaux de bord automatiques. Nous vous recommandons d'activer Lambda Insights pour les tests de performance et les environnements de production. Parmi les indicateurs supplémentaires créés par Lambda Insights, citons ceux `memory_utilization` qui permettent de dimensionner correctement les fonctions Lambda afin d'éviter de payer pour une capacité inutile.

Métriques d'application

Vous pouvez également créer et capturer vos propres métriques d'application à CloudWatch l'aide du format de métrique intégré. Vous pouvez tirer parti des bibliothèques AWS fournies pour le format métrique intégré afin de créer et d'émettre des instructions de format métrique intégré CloudWatch. La fonction de CloudWatch journalisation Lambda intégrée est configurée pour traiter et extraire des instructions au format métrique intégré correctement formatées.

Recherche et analyse des connexions CloudWatch

Une fois que vos journaux et indicateurs ont été capturés dans un format et un emplacement cohérents, vous pouvez les rechercher et les analyser pour améliorer l'efficacité opérationnelle, en plus d'identifier et de résoudre les problèmes. Nous vous recommandons de capturer vos journaux dans un format bien formé (par exemple, JSON) pour faciliter la recherche et l'analyse de vos journaux. La plupart des charges de travail utilisent un ensemble de AWS ressources telles que le réseau, le calcul, le stockage et les bases de données. Dans la mesure du possible, vous devez analyser collectivement les indicateurs et les journaux de ces ressources et les corréler afin de surveiller et de gérer efficacement toutes vos charges de AWS travail.

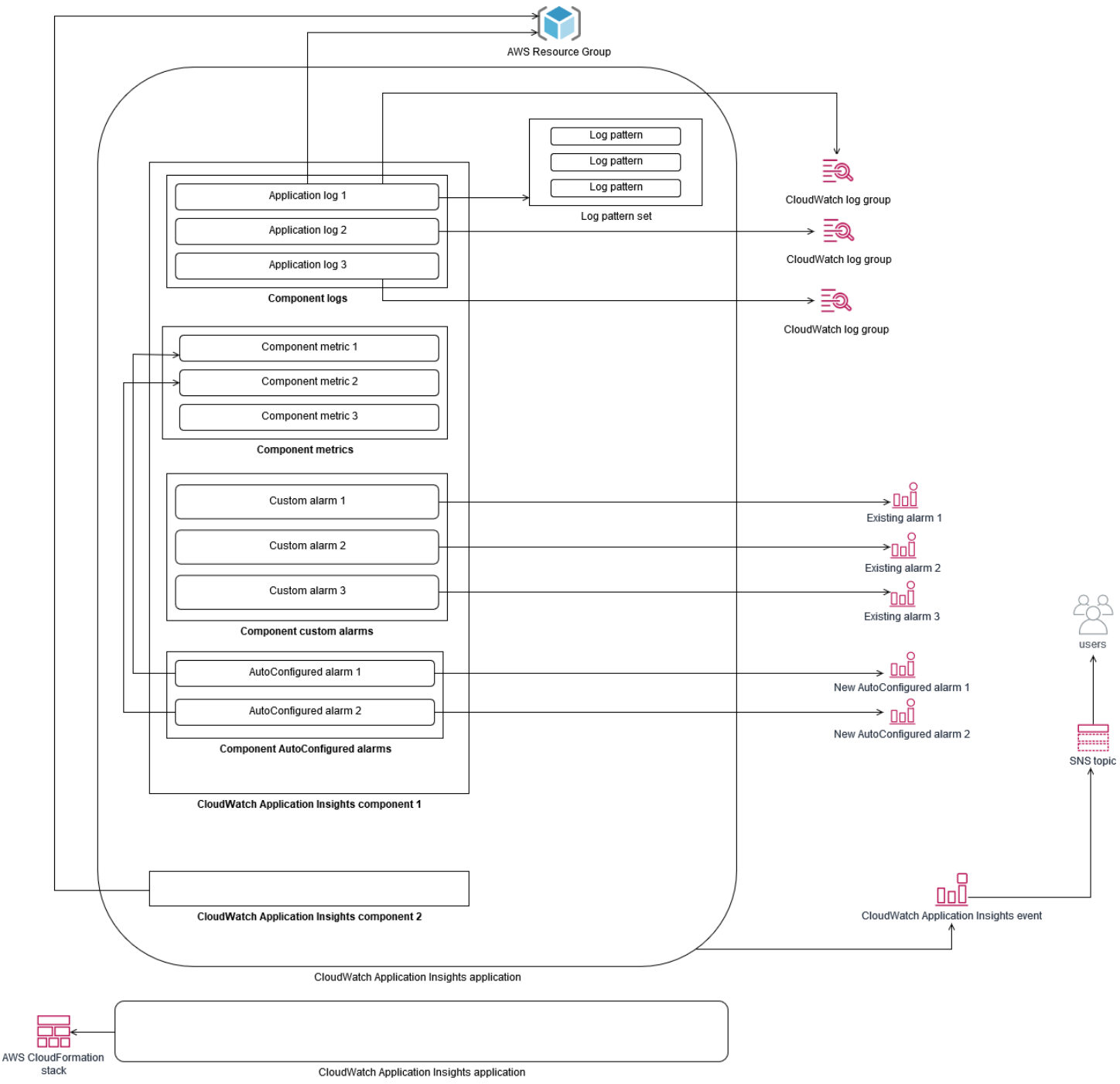
CloudWatch fournit plusieurs fonctionnalités pour aider à analyser les journaux et les métriques, telles que CloudWatch Application Insights pour définir et surveiller collectivement les métriques et les journaux d'une application sur différentes AWS ressources, la détection des CloudWatch anomalies pour détecter les anomalies liées à vos indicateurs, et CloudWatch Log Insights pour rechercher et analyser de manière interactive les données de vos journaux dans CloudWatch les journaux.

Surveillez et analysez collectivement les applications avec CloudWatch Application Insights

Les propriétaires d'applications peuvent utiliser Amazon CloudWatch Application Insights pour configurer la surveillance et l'analyse automatiques des charges de travail. Cela peut être configuré en plus de la surveillance standard au niveau des systèmes configurée pour toutes les charges de travail d'un compte. La mise en place d'une surveillance via CloudWatch Application Insights peut également aider les équipes chargées des applications à s'aligner de manière proactive sur les opérations et à réduire le temps moyen de restauration (MTTR). CloudWatch Application Insights peut aider à réduire les efforts nécessaires pour établir une journalisation et une surveillance au niveau des applications. Il fournit également un cadre basé sur des composants qui aide les équipes à répartir les responsabilités de journalisation et de surveillance.

CloudWatch Application Insights utilise des groupes de ressources pour identifier les ressources qui doivent être surveillées collectivement en tant qu'application. Les ressources prises en charge dans le groupe de ressources deviennent des composants définis individuellement de votre CloudWatch application Application Insights. Chaque composant de votre CloudWatch application Application Insights possède ses propres journaux, métriques et alarmes.

Pour les journaux, vous définissez l'ensemble de modèles de journaux qui doit être utilisé pour le composant et dans votre CloudWatch application Application Insights. Un ensemble de modèles de log est un ensemble de modèles de log à rechercher sur la base d'expressions régulières, avec une sévérité faible, moyenne ou élevée lorsque le modèle est détecté. Pour les métriques, vous choisissez les métriques à surveiller pour chaque composant dans une liste de métriques spécifiques au service et prises en charge. Pour les alarmes, CloudWatch Application Insights crée et configure automatiquement des alarmes de détection standard ou d'anomalie pour les métriques surveillées. CloudWatch Application Insights dispose de configurations automatiques pour les métriques et la capture des journaux pour les technologies décrites dans les journaux et les métriques prises en charge par CloudWatch Application Insights dans la CloudWatch documentation. Le schéma suivant montre les relations entre les composants CloudWatch d'Application Insights et leurs configurations de journalisation et de surveillance. Chaque composant a défini ses propres journaux et mesures à surveiller à l'aide de CloudWatch journaux et de métriques.



EC2 les instances surveillées par CloudWatch Application Insights nécessitent Systems Manager, CloudWatch des agents et des autorisations. Pour plus d'informations à ce sujet, consultez la section Conditions préalables à la configuration d'une application avec CloudWatch Application Insights dans la CloudWatch documentation. CloudWatch Application Insights utilise Systems Manager pour installer et mettre à jour l' CloudWatch agent. Les métriques et les journaux configurés dans CloudWatch Application Insights créent un fichier de configuration d' CloudWatch

agent qui est stocké dans un paramètre Systems Manager avec le `AmazonCloudWatch-ApplicationInsights-SSMParameter` préfixe de chaque composant CloudWatch Application Insights. Cela entraîne l'ajout d'un fichier de configuration d' CloudWatch agent distinct au répertoire de configuration de l' CloudWatch agent sur l' EC2 instance. Une commande Systems Manager est exécutée pour ajouter cette configuration à la configuration active de l' EC2 instance. L'utilisation CloudWatch d'Application Insights n'a aucune incidence sur les paramètres de configuration des CloudWatch agents existants. Vous pouvez utiliser CloudWatch Application Insights en plus de vos propres configurations d' CloudWatch agent au niveau du système et de l'application. Cependant, vous devez vous assurer que les configurations ne se chevauchent pas.

Effectuer une analyse des CloudWatch journaux avec Logs Insights

CloudWatch Logs Insights facilite la recherche dans plusieurs groupes de journaux à l'aide d'un langage de requête simple. Si les journaux de votre application sont structurés au format JSON, CloudWatch Logs Insights découvre automatiquement les champs JSON de vos flux de journaux dans plusieurs groupes de journaux. Vous pouvez utiliser CloudWatch Logs Insights pour analyser les journaux de votre application et de votre système, ce qui enregistre vos requêtes pour une utilisation future. La syntaxe des requêtes pour CloudWatch Logs Insights prend en charge des fonctions telles que l'agrégation avec des fonctions telles que sum (), avg (), count (), min () et max (), qui peuvent être utiles pour le dépannage de vos applications ou l'analyse des performances.

Si vous utilisez le format de métrique intégré pour créer des CloudWatch métriques, vous pouvez interroger vos journaux de format de métrique intégré pour générer des métriques ponctuelles à l'aide des fonctions d'agrégation prises en charge. Cela permet de réduire vos coûts de CloudWatch surveillance en capturant les points de données nécessaires pour générer des mesures spécifiques selon les besoins, au lieu de les capturer activement sous forme de mesures personnalisées. Cela est particulièrement efficace pour les dimensions présentant une cardinalité élevée qui se traduiraient par un grand nombre de mesures. CloudWatch Container Insights adopte également cette approche et capture des données de performance détaillées, mais ne génère CloudWatch des métriques que pour un sous-ensemble de ces données.

Par exemple, l'entrée de mesure intégrée suivante génère uniquement un ensemble limité de CloudWatch mesures à partir des données de mesure capturées dans l'instruction de format de métrique intégrée :

```
{
 "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"
}
```


Cependant, vous pouvez interroger les mesures capturées pour obtenir des informations supplémentaires. Par exemple, vous pouvez exécuter la requête suivante pour voir les 20 derniers modules présentant des erreurs de page mémoire :

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

Exécution d'une analyse des journaux avec Amazon OpenSearch Service

CloudWatch s'intègre à Amazon OpenSearch Service en vous permettant de diffuser les données des journaux des groupes de CloudWatch journaux vers un cluster Amazon OpenSearch Service de votre choix à l'aide d'un filtre d'abonnement. Vous pouvez CloudWatch les utiliser pour la capture et l'analyse des journaux et des métriques principaux, puis les compléter avec Amazon OpenSearch Service pour les cas d'utilisation suivants :

- Contrôle précis de l'accès aux données : Amazon OpenSearch Service vous permet de limiter l'accès aux données au niveau du champ et aide à anonymiser les données contenues dans les champs en fonction des autorisations des utilisateurs. Cela est utile si vous souhaitez obtenir de l'aide pour résoudre les problèmes sans exposer de données sensibles.
- Regroupez et recherchez des journaux sur plusieurs comptes, régions et infrastructures : vous pouvez diffuser vos journaux provenant de plusieurs comptes et régions vers un cluster Amazon OpenSearch Service commun. Vos équipes opérationnelles centralisées peuvent analyser les tendances, les problèmes et effectuer des analyses sur l'ensemble des comptes et des régions. CloudWatch Les journaux de streaming vers Amazon OpenSearch Service vous permettent également de rechercher et d'analyser une application multirégionale dans un emplacement central.
- Envoyez et enrichissez les journaux directement vers Amazon OpenSearch Service à l'aide d' ElasticSearchagents : les composants de votre application et de votre infrastructure technologique peuvent être utilisés OSs s'ils ne sont pas pris en charge par l' CloudWatch agent. Vous souhaiterez peut-être également enrichir et transformer les données des journaux avant qu'elles ne soient expédiées vers votre solution de journalisation. Amazon OpenSearch Service prend en charge les clients Elasticsearch standard tels que les expéditeurs de données de la famille Elastic Beats et Logstash, qui prennent en charge l'enrichissement et la transformation des journaux avant de les envoyer à Amazon Service. OpenSearch
- La solution de gestion des opérations existante utilise une ElasticSearch pile Logstash Kibana (ELK) pour la journalisation et la surveillance. Vous avez peut-être déjà investi de manière significative dans Amazon OpenSearch Service ou Elasticsearch open source, de nombreuses charges de travail étant déjà configurées. Vous pouvez également avoir des tableaux de bord opérationnels créés dans Kibana que vous souhaitez continuer à utiliser.

Si vous ne prévoyez pas d'utiliser de CloudWatch journaux, vous pouvez utiliser des agents, des pilotes de journaux et des bibliothèques compatibles avec Amazon OpenSearch Service (par exemple, Fluent Bit, Fluentd, logstash et Open Distro for ElasticSearch API) pour envoyer vos journaux directement à Amazon Service et les contourner. OpenSearch CloudWatch Cependant, vous devez également implémenter une solution pour capturer les journaux générés par les AWS services. CloudWatch Logs est la principale solution de capture de journaux pour de nombreux AWS services, et plusieurs services créent automatiquement de nouveaux groupes de journaux CloudWatch. Par exemple, Lambda crée un nouveau groupe de journaux pour chaque fonction Lambda. Vous pouvez configurer un filtre d'abonnement pour un groupe de journaux afin de diffuser ses journaux sur Amazon OpenSearch Service. Vous pouvez configurer manuellement un filtre d'abonnement pour chaque groupe de journaux individuel que vous souhaitez diffuser sur Amazon OpenSearch Service. Vous pouvez également déployer une solution qui abonne automatiquement les nouveaux groupes de journaux aux ElasticSearch clusters. Vous pouvez diffuser les journaux vers un ElasticSearch cluster dans le même compte ou dans un compte centralisé. Le streaming des journaux vers un ElasticSearch cluster dans le même compte aide les propriétaires de charges de travail à mieux analyser et prendre en charge leurs charges de travail.

Vous devriez envisager de configurer un ElasticSearch cluster dans un compte centralisé ou partagé pour agréger les journaux entre vos comptes, régions et applications. Par exemple, AWS Control Tower configure un compte Log Archive qui est utilisé pour la journalisation centralisée. Lorsqu'un nouveau compte est créé dans AWS Control Tower, ses AWS Config journaux AWS CloudTrail et journaux sont envoyés dans un compartiment S3 de ce compte centralisé. La journalisation instrumentée par AWS Control Tower est destinée à la journalisation de la configuration, des modifications et des audits.

Pour mettre en place une solution d'analyse centralisée des journaux d'applications avec Amazon OpenSearch Service, vous pouvez déployer un ou plusieurs clusters Amazon OpenSearch Service centralisés sur votre compte de journalisation centralisé et configurer des groupes de journaux dans vos autres comptes pour diffuser les journaux vers les clusters Amazon OpenSearch Service centralisés.

Vous pouvez créer des clusters Amazon OpenSearch Service distincts pour gérer différentes applications ou couches de votre architecture cloud susceptibles d'être réparties sur vos comptes. L'utilisation de clusters Amazon OpenSearch Service distincts vous permet de réduire les risques liés à la sécurité et à la disponibilité, et le fait de disposer d'un cluster Amazon OpenSearch Service commun peut faciliter la recherche et la mise en relation des données au sein d'un même cluster.

Des options alarmantes avec CloudWatch

L'analyse ponctuelle et automatisée des indicateurs importants vous aide à détecter et à résoudre les problèmes avant qu'ils n'affectent vos charges de travail. CloudWatch permet de représenter graphiquement et de comparer facilement plusieurs indicateurs en utilisant plusieurs statistiques sur une période donnée. Vous pouvez l'utiliser CloudWatch pour effectuer une recherche dans tous les indicateurs avec les valeurs de dimension requises afin de trouver les indicateurs dont vous avez besoin pour votre analyse.

Nous vous recommandons de commencer votre approche de capture des métriques en incluant un ensemble initial de métriques et de dimensions à utiliser comme base de référence pour surveiller une charge de travail. Au fil du temps, la charge de travail évolue et vous pouvez ajouter des mesures et des dimensions supplémentaires pour vous aider à mieux l'analyser et à la soutenir. Vos applications ou charges de travail peuvent utiliser plusieurs AWS ressources et avoir leurs propres métriques personnalisées. Vous devez regrouper ces ressources dans un espace de noms pour les identifier plus facilement.

Vous devez également tenir compte de la corrélation entre les données de journalisation et de surveillance afin de pouvoir identifier rapidement les données de journalisation et de surveillance pertinentes pour diagnostiquer des problèmes spécifiques. Vous pouvez utiliser la carte de AWS X-Ray suivi pour corréler les traces, les métriques, les journaux et les alarmes afin de diagnostiquer les problèmes. Vous devriez également envisager d'inclure des dimensions supplémentaires dans les métriques et les identifiants dans les journaux de vos charges de travail afin de vous aider à rechercher et à identifier rapidement les problèmes liés aux systèmes et aux services.

Utilisation d' CloudWatch alarmes pour surveiller et alarmer

Vous pouvez utiliser des CloudWatch alarmes pour réduire la surveillance manuelle de vos charges de travail ou de vos applications. Vous devez commencer par examiner les métriques que vous capturez pour chaque composant de la charge de travail et déterminer les seuils appropriés pour chaque métrique. Assurez-vous d'identifier les membres de l'équipe qui doivent être avertis lorsqu'un seuil est dépassé. Vous devez établir et cibler des groupes de distribution plutôt que des membres individuels de l'équipe.

CloudWatch les alarmes peuvent s'intégrer à votre solution de gestion des services pour créer automatiquement de nouveaux tickets et exécuter des flux de travail opérationnels. Par exemple,

AWS fournit le connecteur AWS de gestion des services pour ServiceNowet Connecteur AWS Service Managementpour vous aider à configurer rapidement les intégrations. Cette approche est essentielle pour garantir que les alarmes déclenchées sont reconnues et alignées sur vos flux de travail opérationnels existants qui peuvent déjà être définis dans ces produits.

Vous pouvez également créer plusieurs alarmes pour la même métrique avec des seuils et des périodes d'évaluation différents, ce qui permet d'établir un processus d'escalade. Par exemple, si vous disposez d'un `OrderQueueDepth` indicateur qui suit les commandes des clients, vous pouvez définir un seuil inférieur sur une courte période moyenne d'une minute pour informer les membres de l'équipe chargée de l'application par e-mail ou par Slack. Vous pouvez également définir une autre alarme pour le même indicateur sur une période plus longue de 15 minutes au même seuil et qui envoie des pages, des e-mails et des notifications à l'équipe d'application et au responsable de l'équipe d'application. Enfin, vous pouvez définir une troisième alarme pour un seuil moyen fixe sur une période de 30 minutes, qui avertit la haute direction et avertit tous les membres de l'équipe préalablement informés. La création de plusieurs alarmes vous permet de prendre différentes mesures en fonction des conditions. Vous pouvez commencer par un processus de notification simple, puis l'ajuster et l'améliorer selon vos besoins.

Utilisation de la détection des CloudWatch anomalies pour la surveillance et l'alarme

Vous pouvez utiliser la détection des CloudWatch anomalies si vous n'êtes pas sûr des seuils à appliquer pour une métrique particulière ou si vous souhaitez qu'une alarme ajuste automatiquement les valeurs de seuil en fonction des valeurs historiques observées. CloudWatch la détection des anomalies est particulièrement utile pour les indicateurs susceptibles d'entraîner des changements d'activité réguliers et prévisibles, par exemple l'augmentation des bons de commande quotidiens destinés à être livrés le jour même avant une heure limite. La détection des anomalies permet des seuils qui s'ajustent automatiquement et peuvent contribuer à réduire le nombre de fausses alarmes. Vous pouvez activer la détection des anomalies pour chaque métrique et statistique, et configurer l'alarme en fonction CloudWatch des valeurs aberrantes.

Par exemple, vous pouvez activer la détection des anomalies pour la `CPUUtilization` métrique et les `AVG` statistiques sur une EC2 instance. La détection des anomalies utilise ensuite jusqu'à 14 jours de données historiques pour créer le modèle d'apprentissage automatique (ML). Vous pouvez créer plusieurs alarmes avec différentes bandes de détection d'anomalies pour établir un processus d'escalade des alarmes, similaire à la création de plusieurs alarmes standard avec des seuils différents.

Pour plus d'informations sur cette section, consultez la section Création d'une CloudWatch alarme basée sur la détection d'anomalies dans la CloudWatch documentation.

Alarme concernant plusieurs régions et comptes

Les propriétaires d'applications et de charges de travail doivent créer des alarmes au niveau de l'application pour les charges de travail couvrant plusieurs régions. Nous vous recommandons de créer des alarmes distinctes pour chaque compte et chaque région dans lesquels votre charge de travail est déployée. Vous pouvez simplifier et automatiser ce processus en utilisant des modèles indépendants CloudFormation StackSets du compte et de la région pour déployer les ressources de l'application avec les alarmes requises. ModèleVous pouvez configurer les actions d'alarme pour cibler un sujet Amazon Simple Notification Service (Amazon SNS) courant, ce qui signifie que la même notification ou action corrective est utilisée quel que soit le compte ou la région.

Dans les environnements multicomptes et multirégionaux, nous vous recommandons de créer des alarmes agrégées pour vos comptes et régions afin de surveiller les problèmes liés aux comptes et aux régions en utilisant CloudFormation StackSets des indicateurs agrégés, tels que la moyenne de `CPUUtilization` toutes les EC2 instances.

Vous devez également envisager de créer des alarmes standard pour chaque charge de travail configurée pour les CloudWatch métriques et les journaux standard que vous capturez. Par exemple, vous pouvez créer une alarme distincte pour chaque EC2 instance qui surveille la métrique d'utilisation du processeur et avertit une équipe des opérations centrales lorsque l'utilisation moyenne du processeur est supérieure à 80 % sur une base quotidienne. Vous pouvez également créer une alarme standard qui surveille l'utilisation moyenne du processeur inférieure à 10 % sur une base quotidienne. Ces alarmes aident l'équipe des opérations centrales à travailler avec des propriétaires de charges de travail spécifiques afin de modifier la taille des EC2 instances lorsque cela est nécessaire.

Automatiser la création d'alarmes à l'aide de balises d' EC2 instance

La création d'un ensemble d'alarmes standard pour vos EC2 instances peut être chronophage, incohérente et source d'erreurs. Vous pouvez accélérer le processus de création d'alarmes en utilisant la amazon-cloudwatch-auto-alarmssolution pour créer automatiquement un ensemble standard d' CloudWatchalarmes pour vos EC2 instances et créer des alarmes personnalisées en

fonction des balises d' EC2 instance. La solution élimine le besoin de créer manuellement des alarmes standard et peut être utile lors d'une migration à grande échelle d' EC2 instances utilisant des outils tels que CloudEndure. Vous pouvez également déployer cette solution CloudFormation StackSets pour prendre en charge plusieurs régions et comptes. Pour plus d'informations, consultez la section Utiliser des balises pour créer et gérer des CloudWatch alarmes Amazon pour les EC2 instances Amazon sur le AWS blog.

Surveillance de la disponibilité des applications et des services

CloudWatch vous aide à surveiller et à analyser les performances et les aspects d'exécution de vos applications et de vos charges de travail. Vous devez également surveiller les aspects de disponibilité et d'accessibilité de vos applications et de vos charges de travail. Vous pouvez y parvenir en utilisant une approche de surveillance active avec les bilans de santé Amazon Route 53 et CloudWatch Synthetics.

Vous pouvez utiliser les contrôles de santé de Route 53 lorsque vous souhaitez surveiller la connectivité à une page Web via HTTP ou HTTPS, ou la connectivité réseau via TCP à un nom ou une adresse IP de système de noms de domaine (DNS) publics. Les contrôles de santé de Route 53 initient des connexions à partir des régions que vous spécifiez toutes les dix ou 30 secondes. Vous pouvez choisir plusieurs régions pour le bilan de santé, chaque bilan de santé est exécuté indépendamment et vous devez choisir au moins trois régions. Vous pouvez rechercher dans le corps de réponse d'une requête HTTP ou HTTPS une sous-chaîne spécifique si elle apparaît dans les 5 120 premiers octets de données renvoyés pour évaluation de l'état de santé. Une requête HTTP ou HTTPS est considérée comme saine si elle renvoie une réponse 2xx ou 3xx. Les bilans de santé Route 53 peuvent être utilisés pour créer un bilan de santé composite en vérifiant l'état des autres bilans de santé. Vous pouvez le faire si vous disposez de plusieurs points de terminaison de service et que vous souhaitez envoyer la même notification lorsque l'un d'entre eux ne fonctionne plus correctement. Si vous utilisez Route 53 pour le DNS, vous pouvez configurer Route 53 pour qu'il bascule vers une autre entrée DNS si un bilan de santé ne fonctionne pas correctement. Pour chaque charge de travail critique, vous devez envisager de configurer des contrôles de santé Route 53 pour les points de terminaison externes essentiels au fonctionnement normal. Les bilans de santé de Route 53 peuvent vous aider à éviter d'écrire une logique de basculement dans vos applications.

CloudWatch synthetics vous permet de définir un canari comme un script permettant d'évaluer l'état et la disponibilité de vos charges de travail. Les canaris sont des scripts écrits en Node.js ou Python qui fonctionnent sur les protocoles HTTP ou HTTPS. Ils créent des fonctions Lambda dans votre compte qui utilisent Node.js ou Python comme cadre. Chaque canari que vous définissez peut effectuer plusieurs appels HTTP ou HTTPS vers différents points de terminaison. Cela signifie que vous pouvez surveiller l'état d'une série d'étapes, telles qu'un cas d'utilisation ou un point de terminaison avec des dépendances en aval. Les canaris créent CloudWatch des métriques qui incluent chaque étape exécutée afin que vous puissiez déclencher une alarme et mesurer les différentes étapes indépendamment. Bien que le développement des canaris nécessite plus de

planification et d'efforts que les bilans de santé de la Route 53, ils vous offrent une approche de suivi et d'évaluation hautement personnalisable. Les îles Canaries prennent également en charge les ressources privées exécutées au sein de votre cloud privé virtuel (VPC), ce qui les rend idéales pour la surveillance de la disponibilité lorsque vous ne disposez pas d'une adresse IP publique pour le point de terminaison. Vous pouvez également utiliser des canaris pour surveiller les charges de travail sur site tant que vous disposez d'une connectivité entre le VPC et le point de terminaison. Cela est particulièrement important lorsque votre charge de travail inclut des terminaux qui existent sur site.

Applications de suivi avec AWS X-Ray

Une demande via votre application peut consister en des appels à des bases de données, à des applications et à des services Web exécutés sur des serveurs locaux, Amazon EC2, des conteneurs ou Lambda. En mettant en œuvre le suivi des applications, vous pouvez rapidement identifier la cause première des problèmes dans vos applications qui utilisent des composants et des services distribués. Vous pouvez l'utiliser AWS X-Raypour suivre les demandes de votre application sur plusieurs composants. X-Ray échantillonne et visualise les demandes sur un graphe de service lorsqu'elles circulent dans les composants de votre application et que chaque composant est représenté sous forme de segment. X-Ray génère des identifiants de suivi afin que vous puissiez corréler une demande lorsqu'elle transite par plusieurs composants, ce qui vous permet de visualiser la demande de bout en bout. Vous pouvez encore améliorer cette fonction en incluant des annotations et des métadonnées pour permettre de rechercher et d'identifier de manière unique les caractéristiques d'une demande.

Nous vous recommandons de configurer et d'instrumenter chaque serveur ou point de terminaison de votre application avec X-Ray. X-Ray est implémenté dans le code de votre application en adressant des appels au service X-Ray. X-Ray propose AWS SDKs également plusieurs langues, y compris des clients instrumentés qui envoient automatiquement des données à X-Ray. The X-Ray SDKs fournit des correctifs aux bibliothèques courantes utilisées pour appeler d'autres services (par exemple, HTTP, MySQL, PostgreSQL ou MongoDB).

X-Ray fournit un démon X-Ray que vous pouvez installer et exécuter sur Amazon EC2 et Amazon ECS pour transmettre des données à X-Ray. X-Ray crée des traces pour votre application qui capturent les données de performance des serveurs et des conteneurs exécutant le daemon X-Ray qui a traité la demande. X-Ray analyse automatiquement vos appels à AWS des services, tels qu'Amazon DynamoDB, sous forme de sous-segments en appliquant des correctifs au SDK. AWS X-Ray peut également s'intégrer automatiquement aux fonctions Lambda.

Si les composants de votre application appellent des services externes qui ne peuvent pas configurer et installer le daemon X-Ray ou instrumenter le code, vous pouvez créer des sous-segments pour encapsuler les appels aux services externes. X-Ray met en corrélation les CloudWatch journaux et les métriques avec les traces de votre application si vous utilisez le Kit SDK AWS X-Ray pour Java, ce qui signifie que vous pouvez rapidement analyser les métriques et les journaux associés aux demandes.

Déploiement du daemon X-Ray pour suivre les applications et les services sur Amazon EC2

Vous devez installer et exécuter le daemon X-Ray sur les EC2 instances sur lesquelles s'exécutent les composants de votre application ou vos microservices. Vous pouvez utiliser un script de données utilisateur pour déployer le daemon X-Ray lorsque des EC2 instances sont provisionnées ou vous pouvez l'inclure dans le processus de génération de l'AMI si vous créez le vôtre. AMIs Cela peut être particulièrement utile lorsque les EC2 instances sont éphémères.

Vous devez utiliser State Manager pour vous assurer que le daemon X-Ray est toujours installé sur vos EC2 instances. Pour les instances Amazon EC2 Windows, vous pouvez utiliser le RunPowerShellScript document Systems Manager AWS- pour exécuter le script Windows qui télécharge et installe l'agent X-Ray. Pour les EC2 instances sous Linux, vous pouvez utiliser le RunShellScript document AWS- pour exécuter le script Linux qui télécharge et installe l'agent en tant que service.

Vous pouvez utiliser le RunRemoteScript document Systems Manager AWS pour exécuter le script dans un environnement multi-comptes. Vous devez créer un compartiment S3 accessible depuis tous vos comptes et nous vous recommandons de créer un compartiment S3 avec une politique de compartiment basée sur l'organisation si vous en utilisez. AWS Organizations Vous téléchargez ensuite les scripts dans le compartiment S3, mais assurez-vous que le rôle IAM de vos EC2 instances est autorisé à accéder au compartiment et aux scripts.

Vous pouvez également configurer State Manager pour associer les scripts aux EC2 instances sur lesquelles l'agent X-Ray est installé. Étant donné que toutes vos EC2 instances ne nécessitent peut-être pas ou n'utilisent pas X-Ray, vous pouvez cibler l'association avec des balises d'instance. Par exemple, vous pouvez créer l'association State Manager en fonction de la présence de `InstallAWSXRayDaemonWindows` ou de `InstallAWSXRayDaemonLinux` balises.

Déploiement du daemon X-Ray pour suivre les applications et les services sur Amazon ECS ou Amazon EKS

Vous pouvez déployer le daemon X-Ray en tant que conteneur annexe pour les charges de travail basées sur des conteneurs telles qu'Amazon ECS ou Amazon EKS. Vos conteneurs d'applications peuvent ensuite se connecter à votre conteneur de sidecar grâce à la liaison de conteneurs si vous utilisez Amazon ECS, ou le conteneur peut se connecter directement au conteneur de sidecar sur localhost si vous utilisez le mode réseau awsvpc.

Pour Amazon EKS, vous pouvez définir le démon X-Ray dans la définition du pod de votre application, puis votre application peut se connecter au démon via localhost sur le port de conteneur que vous avez spécifié.

Configuration de Lambda pour suivre les demandes adressées à X-Ray

Votre application peut inclure des appels aux fonctions Lambda. Il n'est pas nécessaire d'installer le démon X-Ray pour Lambda car le processus du démon est entièrement géré par Lambda et ne peut pas être configuré par l'utilisateur. Vous pouvez l'activer pour votre fonction Lambda en utilisant AWS Management Console et en cochant l'option Active Tracing dans la console X-Ray.

Pour une instrumentation plus poussée, vous pouvez associer le SDK X-Ray à votre fonction Lambda pour enregistrer les appels sortants et ajouter des annotations ou des métadonnées.

Instrumentation de vos applications pour X-Ray

Vous devez évaluer le SDK X-Ray qui s'aligne sur le langage de programmation de votre application et classer tous les appels que votre application fait à d'autres systèmes. Passez en revue les clients fournis par la bibliothèque que vous avez choisie et vérifiez si le SDK peut automatiquement contrôler le suivi de la demande ou de la réponse de votre application. Déterminez si les clients fournis par le SDK peuvent être utilisés pour d'autres systèmes en aval. Pour les systèmes externes auxquels votre application fait appel et que vous ne pouvez pas instrumenter avec X-Ray, vous devez créer des sous-segments personnalisés pour les capturer et les identifier dans vos informations de suivi.

Lorsque vous instrumentez votre application, veillez à créer des annotations pour vous aider à identifier et à rechercher des demandes. Par exemple, votre application peut utiliser un identifiant pour les clients, par exemple`customer id`, ou segmenter différents utilisateurs en fonction de leur rôle dans l'application.

Vous pouvez créer un maximum de 50 annotations pour chaque trace, mais vous pouvez créer un objet de métadonnées contenant un ou plusieurs champs tant que le document segmenté ne dépasse pas 64 kilo-octets. Vous devez utiliser des annotations de manière sélective pour localiser les informations et utiliser l'objet de métadonnées pour fournir davantage de contexte afin de faciliter le dépannage de la demande une fois celle-ci localisée.

Configuration des règles d'échantillonnage X-Ray

En personnalisant les règles d'échantillonnage, vous pouvez contrôler la quantité de données que vous enregistrez et modifier le comportement d'échantillonnage sans modifier ni redéployer votre code. Les règles d'échantillonnage indiquent au SDK X-Ray le nombre de demandes à enregistrer pour un ensemble de critères. Par défaut, le SDK X-Ray enregistre la première demande chaque seconde et 5 % des demandes supplémentaires. Une demande par seconde est le réservoir. Ceci garantit qu'au moins une trace est enregistrée chaque seconde aussi longtemps que le service traite les demandes. Cinq pour cent est le taux auquel les demandes supplémentaires sont échantillonnées au-delà de la taille du réservoir.

Vous devez revoir et mettre à jour la configuration par défaut afin de déterminer une valeur appropriée pour votre compte. Vos exigences peuvent varier selon les environnements de développement, de test, de test de performance et de production. Certaines applications nécessitent peut-être leurs propres règles d'échantillonnage en fonction de la quantité de trafic qu'elles reçoivent ou de leur niveau de criticité. Vous devez commencer par une base de référence et réévaluer régulièrement si la référence répond à vos exigences.

Tableaux de bord et visualisations avec CloudWatch

Les tableaux de bord vous aident à vous concentrer rapidement sur les domaines présentant un intérêt pour les applications et les charges de travail. CloudWatchfournit des tableaux de bord automatiques et vous pouvez également créer facilement des tableaux de bord utilisant CloudWatch des métriques. CloudWatch les tableaux de bord fournissent plus d'informations que l'affichage des indicateurs isolément, car ils vous aident à corréler plusieurs indicateurs et à identifier les tendances. Par exemple, un tableau de bord qui inclut les commandes reçues, la mémoire, l'utilisation du processeur et les connexions aux bases de données peut vous aider à corréler l'évolution des indicateurs de charge de travail entre plusieurs AWS ressources lorsque le nombre de commandes augmente ou diminue.

Vous devez créer des tableaux de bord au niveau du compte et de l'application pour surveiller les charges de travail et les applications. Vous pouvez commencer en utilisant des tableaux de bord CloudWatch automatiques, qui sont des tableaux de bord de AWS niveau de service préconfigurés avec des métriques spécifiques aux services. Les tableaux de bord de service automatiques affichent toutes les CloudWatch mesures standard du service. Les tableaux de bord automatiques représentent graphiquement toutes les ressources utilisées pour chaque indicateur de service et vous aident à identifier rapidement les ressources exceptionnelles sur votre compte. Cela peut vous aider à identifier les ressources dont le taux d'utilisation est élevé ou faible, ce qui peut vous aider à optimiser vos coûts.

Création de tableaux de bord multiservices

Vous pouvez créer des tableaux de bord interservices en consultant le tableau de bord automatique des niveaux de service d'un AWS service et en utilisant l'option Ajouter au tableau de bord dans le menu Actions. Vous pouvez ensuite ajouter des métriques provenant d'autres tableaux de bord automatiques à votre nouveau tableau de bord et supprimer des métriques pour affiner le focus du tableau de bord. Vous devez également ajouter vos propres indicateurs personnalisés pour suivre les observations clés (par exemple, les commandes reçues ou les transactions par seconde). La création de votre propre tableau de bord multiservice personnalisé vous permet de vous concentrer sur les indicateurs les plus pertinents pour votre charge de travail. Nous vous recommandons de créer des tableaux de bord interservices au niveau du compte qui couvrent les indicateurs clés et affichent toutes les charges de travail d'un compte.

Si vous disposez d'un espace de bureau central ou d'un espace commun pour vos équipes chargées des opérations cloud, vous pouvez afficher le CloudWatch tableau de bord sur un grand écran de télévision en mode plein écran avec actualisation automatique.

Création de tableaux de bord spécifiques à une application ou à une charge de travail

Nous vous recommandons de créer des tableaux de bord spécifiques aux applications et aux charges de travail qui mettent l'accent sur les indicateurs et les ressources clés pour chaque application ou charge de travail critique de votre environnement de production. Les tableaux de bord spécifiques aux applications et aux charges de travail se concentrent sur les indicateurs personnalisés de votre application ou de votre charge de travail et sur les indicateurs de AWS ressources importants qui influencent leurs performances.

Vous devez évaluer et personnaliser régulièrement les tableaux de bord de votre CloudWatch application ou de votre charge de travail afin de suivre les indicateurs clés après la survenue d'incidents. Vous devez également mettre à jour les tableaux de bord spécifiques à l'application ou à la charge de travail lorsque des fonctionnalités sont introduites ou supprimées. Les mises à jour des tableaux de bord spécifiques à la charge de travail et aux applications devraient être une activité requise pour l'amélioration continue de la qualité, en plus de la journalisation et de la surveillance.

Création de tableaux de bord entre comptes ou entre régions

AWS les ressources sont principalement régionales et les métriques, les alarmes et les tableaux de bord sont spécifiques à la région dans laquelle les ressources sont déployées. Cela peut vous obliger à modifier les régions pour afficher les métriques, les tableaux de bord et les alarmes pour les charges de travail et les applications interrégionales. Si vous séparez vos applications et vos charges de travail sur plusieurs comptes, vous devrez peut-être également vous authentifier à nouveau et vous reconnecter à chaque compte. Cependant, il CloudWatch prend en charge l'affichage des données entre comptes et entre régions à partir d'un seul compte, ce qui signifie que vous pouvez consulter les métriques, les alarmes, les tableaux de bord et les widgets de journal dans un seul compte et une seule région. Cela est très utile si vous disposez d'un compte de journalisation et de surveillance centralisé.

Les propriétaires de comptes et les responsables des équipes d'application doivent créer des tableaux de bord pour les applications interrégionales spécifiques au compte afin de surveiller

efficacement les indicateurs clés dans un emplacement centralisé. CloudWatchles tableaux de bord prennent automatiquement en charge les widgets interrégionaux, ce qui signifie que vous pouvez créer un tableau de bord qui inclut des statistiques provenant de plusieurs régions sans autre configuration.

Le widget CloudWatch Logs Insights constitue une exception importante, car les données du journal ne peuvent être affichées que pour le compte et la région auxquels vous êtes actuellement connecté. Vous pouvez créer des métriques spécifiques à une région à partir de vos journaux à l'aide de filtres métriques et ces métriques peuvent être affichées sur un tableau de bord interrégional. Vous pouvez ensuite passer à la région spécifique lorsque vous devez analyser ces journaux de manière plus approfondie.

Les équipes opérationnelles doivent créer un tableau de bord centralisé qui surveille les indicateurs importants entre comptes et entre régions. Par exemple, vous pouvez créer un tableau de bord multi-comptes qui inclut l'utilisation globale du processeur dans chaque compte et région. Vous pouvez également utiliser les mathématiques métriques pour agréger et intégrer les données de plusieurs comptes et régions.

Utiliser les mathématiques métriques pour affiner l'observabilité et les alarmes

Vous pouvez utiliser les mathématiques des métriques pour calculer les métriques dans des formats et des expressions adaptés à vos charges de travail. Les mesures calculées peuvent être enregistrées et affichées sur un tableau de bord à des fins de suivi. Par exemple, les mesures de volume standard d'Amazon EBS indiquent le nombre d'opérations de lecture (`VolumeReadOps`) et d'écriture (`VolumeWriteOps`) effectuées sur une période donnée.

Cependant, AWS fournit des directives sur les performances des volumes Amazon EBS en termes d'IOPS. Vous pouvez représenter graphiquement et calculer les IOPS pour votre volume Amazon EBS en mathématiques métriques en ajoutant `VolumeReadOps` `VolumeWriteOps` puis en divisant par la période choisie pour ces statistiques.

Dans cet exemple, nous additionnons les IOPS de la période, puis nous les divisons par la durée de la période pour obtenir les IOPS. Vous pouvez ensuite définir une alarme pour cette expression mathématique métrique afin de vous avertir lorsque les IOPS de votre volume approchent de la capacité maximale pour son type de volume. Pour plus d'informations et des exemples sur l'utilisation des mathématiques métriques pour surveiller les systèmes de fichiers Amazon Elastic File System

(Amazon EFS) à l'aide de CloudWatch métriques, consultez Amazon CloudWatch Metric Math simplifie la surveillance en temps quasi réel de vos systèmes de fichiers Amazon EFS et plus encore sur le AWS blog.

Utilisation de tableaux de bord automatiques pour Amazon ECS, Amazon EKS et Lambda CloudWatchContainer avec Insights et Lambda Insights CloudWatch

CloudWatch Container Insights crée des tableaux de bord dynamiques et automatiques pour les charges de travail des conteneurs exécutées sur Amazon ECS et Amazon EKS. Vous devez activer Container Insights pour pouvoir observer le processeur, la mémoire, le disque, le réseau et obtenir des informations de diagnostic telles que les échecs de redémarrage des conteneurs. Container Insights génère des tableaux de bord dynamiques que vous pouvez filtrer rapidement au niveau du cluster, de l'instance ou du nœud du conteneur, du service, de la tâche, du pod et du conteneur individuel. Container Insights est configuré au niveau du cluster et du nœud ou de l'instance de conteneur en fonction du AWS service.

À l'instar de Container Insights, CloudWatch Lambda Insights crée des tableaux de bord dynamiques et automatiques pour vos fonctions Lambda. Cette solution collecte, agrège et résume les métriques au niveau du système, notamment le temps processeur, la mémoire, le disque et le réseau. Il collecte, agrège et résume également les informations de diagnostic telles que les démarrages à froid et les arrêts des opérateurs Lambda pour vous aider à isoler et à résoudre rapidement les problèmes liés à vos fonctions Lambda. Lambda est activé au niveau de la fonction et ne nécessite aucun agent.

Container Insights et Lambda Insights vous aident également à passer rapidement aux journaux des applications ou des performances, aux traces X-Ray et à une carte des services pour visualiser les charges de travail de vos conteneurs. Ils utilisent tous deux le format de métrique CloudWatch intégré pour capturer CloudWatch les métriques et les journaux de performance.

Vous pouvez créer un tableau de CloudWatch bord partagé pour votre charge de travail qui utilise les métriques capturées par Container Insights et Lambda Insights. Vous pouvez le faire en filtrant et en consultant le tableau de bord automatique via CloudWatch Container Insights, puis en choisissant l'option Ajouter au tableau de bord qui vous permet d'ajouter les métriques affichées à un tableau de CloudWatch bord standard. Vous pouvez ensuite supprimer ou personnaliser les métriques et ajouter d'autres métriques pour représenter correctement votre charge de travail.

CloudWatch intégration avec les AWS services

AWS fournit de nombreux services qui incluent des options de configuration supplémentaires pour la journalisation et les métriques. Ces services vous permettent souvent de configurer les CloudWatch journaux pour la sortie des journaux et CloudWatch les métriques pour la sortie des métriques. L'infrastructure sous-jacente utilisée pour fournir ces services est gérée par AWS et est inaccessible, mais vous pouvez utiliser les options de journalisation et de métrique pour vos services fournis afin d'obtenir des informations supplémentaires et de résoudre les problèmes. Par exemple, vous pouvez publier des journaux de flux VPC sur CloudWatch, ou vous pouvez également configurer des instances Amazon Relational Database Service (Amazon RDS) sur lesquelles publier des journaux. CloudWatch

La plupart AWS des services enregistrent leurs appels d'API avec intégration à AWS CloudTrail. CloudTrail prend également en charge l'intégration avec CloudWatch Logs, ce qui signifie que vous pouvez rechercher et analyser l'activité dans les AWS services. Vous pouvez également utiliser Amazon EventBridge pour créer et configurer l'automatisation et les notifications avec des règles d'événements pour des actions spécifiques effectuées dans les AWS services. Certains services s'intègrent directement à EventBridge. Vous pouvez également créer des événements diffusés via CloudTrail.

Amazon Managed Grafana pour les tableaux de bord et la visualisation

Amazon Managed Grafana peut être utilisé pour observer et visualiser vos AWS charges de travail. Amazon Managed Grafana vous aide à visualiser et à analyser vos données opérationnelles à grande échelle. Grafana est une plateforme d'analyse open source qui vous permet d'interroger, de visualiser, d'alerter et de comprendre vos indicateurs, quel que soit l'endroit où ils sont stockés. Amazon Managed Grafana est particulièrement utile si votre entreprise utilise déjà Grafana pour visualiser les charges de travail existantes et si vous souhaitez étendre la couverture aux charges de travail. AWS Vous pouvez utiliser Amazon Managed Grafana en l' CloudWatch ajoutant comme source de données, ce qui signifie que vous pouvez créer des visualisations à l'aide de métriques. CloudWatch Amazon Managed Grafana prend en charge AWS Organizations et vous pouvez centraliser les tableaux de bord à l'aide de CloudWatch statistiques provenant de plusieurs comptes et régions.

Le tableau suivant présente les avantages et les considérations liés à l'utilisation d'Amazon Managed Grafana plutôt que CloudWatch pour les tableaux de bord. Une approche hybride peut être appropriée en fonction des différentes exigences de vos utilisateurs finaux, de vos charges de travail et de vos applications.

Créez des visualisations et des tableaux de bord qui s'intègrent aux sources de données prises en charge par Amazon Managed Grafana et le logiciel libre Grafana	Amazon Managed Grafana vous aide à créer des visualisations et des tableaux de bord à partir de nombreuses sources de données différentes, y compris des métriques. CloudWatch Amazon Managed Grafana inclut un certain nombre de sources de données intégrées qui couvrent les AWS services, les logiciels open source et les logiciels COTS. Pour plus d'informations à ce sujet, consultez la section Sources de données intégrées dans la documentation Amazon Managed Grafana. Vous pouvez également ajouter la prise en charge d'un plus grand nombre de sources de données en mettant à niveau votre

	espace de travail vers Grafana Enterprise. Grafana prend également en charge les plugins de source de données qui vous permetten t de communiquer avec différents systèmes externes. CloudWatch les tableaux de bord nécessitent une CloudWatch métrique ou une requête CloudWatch Logs Insights pour que les données soient affichées sur un CloudWatch tableau de bord.
Gérez l'accès à votre solution de tableau de bord séparément de l'accès à votre AWS compte	Amazon Managed Grafana nécessite l'utilisa tion de AWS IAM Identity Center (IAM Identity Center) ainsi que AWS Organizations pour l'authentification et l'autorisation. Cela vous permet d'authentifier les utilisateurs auprès de Grafana en utilisant la fédération d'identité que vous utilisez peut-être déjà avec IAM Identity Center ou. AWS Organizations Toutefois , si vous n'utilisez pas IAM Identity Center AWS Organizations, celui-ci est configuré dans le cadre du processus de configuration d'Amazon Managed Grafana. Cela peut poser problème si votre organisation a limité l'utilisa tion d'IAM Identity Center ou AWS Organizat ions.

Ingérez et accédez aux données de plusieurs comptes et régions grâce AWS Organizations à l'intégration	Amazon Managed Grafana s'intègre AWS Organizations pour vous permettre de lire des données provenant de AWS sources telles qu' CloudWatch Amazon OpenSearch Service sur tous vos comptes. Cela permet de créer des tableaux de bord qui affichent des visualisations à l'aide des données de vos comptes. Pour activer automatiquement l'accès aux données AWS Organizations, vous devez configurer votre espace de travail Amazon Managed Grafana dans le compte de AWS Organizations gestion. Cela n'est pas recommandé sur la base des AWS Organizations meilleures pratiques relatives au compte de gestion. En revanche, il prend CloudWatch également en charge les tableaux de bord entre comptes et entre régions pour les métriques. CloudWatch
Utilisez des widgets de visualisation avancés et des définitions Grafana disponibles dans la communauté open source	Grafana fournit une vaste collection de visualisations que vous pouvez utiliser lors de la création de vos tableaux de bord. Il existe également une vaste bibliothèque de tableaux de bord fournis par la communauté que vous pouvez modifier et réutiliser selon vos besoins.
Utilisez des tableaux de bord avec les déploiements Grafana nouveaux et existants	Si vous utilisez déjà Grafana, vous pouvez importer et exporter des tableaux de bord à partir de vos déploiements Grafana et les personnaliser pour les utiliser dans Amazon Managed Grafana. Amazon Managed Grafana vous permet de standardiser Grafana comme solution de tableau de bord.

Configuration et configuration avancées pour les espaces de travail, les autorisations et les sources de données	Amazon Managed Grafana vous permet de créer plusieurs espaces de travail Grafana dotés de leur propre ensemble de sources de données, d'utilisateurs et de politiques configurés. Cela peut vous aider à répondre à des exigences de cas d'utilisation plus avancées, ainsi qu'à des configurations de sécurité avancées. Les fonctionnalités avancées peuvent obliger vos équipes à développer leur expérience avec Grafana si elles ne possèdent pas déjà ces compétences.

Conception et mise en œuvre de la journalisation et de la surveillance avec CloudWatch FAQ

Cette section fournit des réponses aux questions fréquemment posées sur la conception et la mise en œuvre d'une solution de journalisation et de surveillance avec CloudWatch.

Où puis-je stocker mes fichiers CloudWatch de configuration ?

L' CloudWatch agent pour Amazon EC2 peut appliquer plusieurs fichiers de configuration stockés dans le répertoire CloudWatch de configuration. Idéalement, vous devez stocker votre CloudWatch configuration sous la forme d'un ensemble de fichiers, car vous pouvez contrôler les versions et les réutiliser sur plusieurs comptes et environnements. Pour plus d'informations à ce sujet, consultez la Gestion des CloudWatch configurations section de ce guide. Vous pouvez également stocker vos fichiers de configuration dans un référentiel sur GitHub et automatiser la récupération des fichiers de configuration lorsqu'une nouvelle EC2 instance est mise en service.

Comment créer un ticket dans ma solution de gestion des services lorsqu'une alarme est déclenchée ?

Vous intégrez votre système de gestion des services à une rubrique Amazon Simple Notification Service (Amazon SNS) et vous configurez CloudWatch l'alarme pour avertir la rubrique SNS lorsqu'une alarme est déclenchée. Votre système intégré reçoit le message SNS et peut créer un ticket à l'aide de vos systèmes de gestion des services APIs ou SDKs.

Comment puis-je capturer CloudWatch des fichiers journaux dans mes conteneurs ?

Les tâches Amazon ECS et les pods Amazon EKS peuvent être configurés pour envoyer automatiquement les sorties STDOUT et STDERR à. CloudWatch L'approche recommandée pour la journalisation des applications conteneurisées consiste à faire en sorte que les conteneurs envoient leur sortie à STDOUT et STDERR. Cela est également abordé dans le manifeste de l'application Twelve-Factor.

Toutefois, si vous souhaitez envoyer des fichiers journaux spécifiques, CloudWatch vous pouvez monter un volume dans votre espace Amazon EKS ou dans votre définition de tâche Amazon ECS

sur lequel votre application écrira ses fichiers de lot et utiliser un conteneur annexe pour Fluentd ou Fluent Bit pour envoyer les journaux. CloudWatch Vous devriez envisager de lier symboliquement un fichier journal spécifique de votre conteneur à `/dev/stdout` et`/dev/stderr`. Pour plus d'informations à ce sujet, consultez Afficher les journaux d'un conteneur ou d'un service dans la documentation Docker.

Comment puis-je surveiller les problèmes de santé liés aux AWS services ?

Vous pouvez utiliser le AWS Health Dashboardpour surveiller les AWS problèmes de santé. Vous pouvez également consulter le aws-health-tools GitHub référentiel pour des exemples de solutions d'automatisation liées aux événements AWS médicaux.

Comment créer une CloudWatch métrique personnalisée lorsqu'aucun agent n'est disponible ?

Vous pouvez utiliser le format de métrique intégré pour ingérer des métriques dans CloudWatch. Vous pouvez également utiliser le AWS SDK (par exemple, put_metric_data), AWS CLI (par exemple,) ou l' AWS API (par exemple, put-metric-data) pour créer des métriques personnalisées. PutMetricData Vous devez réfléchir à la manière dont toute logique personnalisée sera maintenue à long terme. Une approche consisterait à utiliser Lambda avec support intégré au format métrique pour créer vos métriques, ainsi qu'une règle de planification CloudWatch des événements pour établir la période de la métrique.

Comment intégrer mes outils de journalisation et de surveillance existants AWS ?

Vous devez vous référer aux instructions fournies par le fournisseur du logiciel ou du service pour l'intégration à AWS. Vous pouvez peut-être utiliser un logiciel agent, un SDK ou une API fournis pour envoyer des journaux et des métriques à leur solution. Vous pouvez également utiliser une solution open source, telle que Fluentd ou Fluent Bit, configurée selon les spécifications du fournisseur. Vous pouvez également utiliser les filtres d'abonnement au AWS SDK et CloudWatch aux journaux avec Lambda et Kinesis Data Streams pour créer des processeurs de journaux et des expéditeurs personnalisés. Enfin, vous devez également réfléchir à la manière dont vous allez intégrer le logiciel si vous utilisez plusieurs comptes et régions.

Ressources

Introduction

- AWS Well-Architected

Résultats commerciaux ciblés

- logging-monitoring-apg-guide-exemples
- Six avantages du cloud computing

Planification de votre CloudWatch déploiement

- Terminologie et concepts relatifs àAWS Organizations
- AWS Systems Manager Configuration rapide
- Collecte de métriques et de journaux à partir d' EC2 instances Amazon et de serveurs sur site avec l'agent CloudWatch
- cloudwatch-config-s3-bucket.yaml
- Créez le fichier de configuration de CloudWatch l'agent à l'aide de l'assistant
- Enterprise DevOps : pourquoi vous devez exécuter ce que vous créez
- Exporter les données du journal vers Amazon S3
- Contrôle d'accès précis dans Amazon Service OpenSearch
- Quotas Lambda
- Création ou modification manuelle du fichier de configuration de CloudWatch l'agent
- Traitement en temps réel des données du journal avec les abonnements
- Des outils sur lesquels s'appuyer AWS

Configuration de l' CloudWatch agent pour les EC2 instances et les serveurs locaux

- Dimensions EC2 métriques d'Amazon

- Instances de performance éclatantes
- CloudWatch ensembles de mesures prédéfinis par l'agent
- Collectez des métriques de processus avec le plugin procstat
- Configuration de l' CloudWatch agent pour procstat
- Gérez la surveillance détaillée de vos EC2 instances
- Ingestion de journaux à haute cardinalité et génération de métriques avec CloudWatch un format de métrique intégré
- Utilisation de groupes de journaux et de flux de journaux
- Répertoriez CloudWatch les métriques disponibles pour vos instances
- PutLogEvents
- Récupérez des métriques personnalisées avec collectd
- Récupérez des métriques personnalisées avec StatsD

CloudWatch approches d'installation d'agents pour Amazon EC2 et les serveurs sur site

- Créer le rôle de service IAM requis pour Systems Manager dans les environnements hybrides et multicloud
- Création d'une activation d'instance gérée pour un environnement hybride
- Création de rôles et d'utilisateurs IAM à utiliser avec l'agent CloudWatch
- Téléchargez et configurez l' CloudWatch agent à l'aide de la ligne de commande
- Comment configurer les serveurs locaux qui utilisent l'agent Systems Manager et l' CloudWatch agent unifié pour n'utiliser que des informations d'identification temporaires ?
- Conditions préalables pour les opérations relatives aux ensembles de piles
- Utilisation d'instances ponctuelles

Journalisation et surveillance sur Amazon ECS

- amazon-cloudwatch-logs-for-bit fluide
- CloudWatchMétriques Amazon ECS
- Statistiques d'Amazon ECS Container Insights

- Agent de conteneur Amazon ECS
- Types de lancement d'Amazon ECS
- Déploiement de l' CloudWatch agent pour collecter des métriques EC2 au niveau de l'instance sur Amazon ECS
- ecs_cluster_with_cloudwatch_linux.yaml
- ecs_cw_emf_example
- ecs_firelense_emf_example
- ecs-task-nginx-firelense.json
- Récupération des métadonnées AMI optimisées pour Amazon ECS
- Utilisation du pilote de journal awslogs
- Utilisation des bibliothèques clientes pour générer des journaux au format métrique intégrés

Journalisation et surveillance dans Amazon EKS

- Journalisation de plan de contrôle d'Amazon EKS
- amazon_eks_managed_node_group_launch_config.yaml
- Nœuds Amazon EKS
- amazon-eks-nodegroup.yaml
- Contrat de niveau de service Amazon EKS
- Container Insights Prometheus : surveillance des métriques
- Métriques du plan de contrôle avec Prometheus
- Exploitation forestière de Fargate
- Fluent Bit pour Amazon EKS sur Fargate
- Comment capturer les journaux d'applications lors de l'utilisation d'Amazon EKS sur Fargate
- Installation de l' CloudWatch agent pour collecter les métriques Prometheus
- Installation du serveur Kubernetes Metrics
- kubernetes/tableau de bord
- Autoscaleur automatique Kubernetes Horizontal Pod
- Composants du plan de contrôle Kubernetes
- Capsules Kubernetes
- Support du modèle de lancement

- Groupes de nœuds gérés
- Comportement de mise à jour des nœuds
- serveur de métriques
- Surveillance d'Amazon EKS sur Fargate à l'aide de Prometheus et Grafana
- prometheus jmx
- prometheus/jmx_exporter
- Supprimer des sources Prometheus supplémentaires et importer ces indicateurs
- Nœuds autogérés
- Envoyer des journaux à CloudWatch Logs
- Configurer FluentD en tant que pour envoyer des journaux DaemonSet à Logs CloudWatch
- Configurer un Java/JMX exemple de charge de travail sur Amazon EKS et Kubernetes
- Tutoriel pour ajouter une nouvelle cible Prometheus Scrape : Prometheus API Server metrics
- Autoscaler à nacelle verticale

Journalisation et statistiques pour AWS Lambda

- Erreurs d'invocation Lambda
- logging — Fonctionnalité de journalisation pour Python
- Utilisation des bibliothèques clientes pour générer des journaux au format métrique intégrés
- Utilisation des métriques de la fonction Lambda

Recherche et analyse des connexions CloudWatch

- La famille Beats
- Logstash élastique
- Pile élastique
- Streaming : CloudWatch enregistre les données vers Amazon OpenSearch Service

Des options alarmantes avec CloudWatch

- amazon-cloudwatch-auto-alarms

- AWS Connecteur de gestion des services pour Jira Service Management Cloud
- AWS Connecteur de gestion des services pour le centre de données Jira Service Management
- AWS Connecteur de gestion des services pour ServiceNow

Surveillance de la disponibilité des applications et des services

- Configuration du basculement DNS

Applications de traçage avec AWS X-Ray

- Mise en réseau des tâches Amazon ECS
- Configuration des règles d'échantillonnage dans la console X-Ray
- Exécuter des PowerShell commandes ou des scripts Windows
- Exécution du daemon X-Ray sur Amazon EC2
- Envoi de données de suivi à X-Ray
- Graphe de service dans X-Ray

Tableaux de bord et visualisations avec CloudWatch

- Amazon CloudWatch Metric Math simplifie la surveillance en temps quasi réel de vos systèmes de fichiers Amazon EFS
- Configuration de CloudWatch Container Insights
- Utilisation des mathématiques métriques

CloudWatch intégration avec les AWS services

- AWS CloudTrail services et intégrations pris en charge
- Événements provenant Services AWS d'Amazon EventBridge
- Événements relatifs aux services AWS organisés via AWS CloudTrail
- Surveillance des fichiers CloudTrail journaux avec CloudWatch Logs
- Publication des journaux de base de données dans CloudWatch Logs

- Publication des journaux de flux dans CloudWatch Logs

Amazon Managed Grafana pour les tableaux de bord et la visualisation

- Bonnes pratiques pour le compte de gestion dans AWS Organizations
- Sources de données intégrées pour Amazon Managed Grafana
- Tableaux de bord entre comptes et entre régions dans CloudWatch
- Plug-ins Grafana

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un fil RSS.

Modification	Description	Date
Informations de journalisation mises à jour	Mise à jour de la section sur la journalisation pour AWS Lambda.	17 avril 2023
Informations de configuration mises à jour	Mise à jour et renommage de la section sur la création et le stockage des CloudWatch configurations.	9 février 2023
Informations sur les métriques mises à jour	Les informations sur les métriques d'application personnalisées ont été mises à jour dans la section Mesures pour Amazon ECS.	31 janvier 2023
Notices d'aperçu supprimées	Amazon Managed Grafana est généralement disponible.	25 mai 2022
Section supprimée	CloudWatch Les métriques du SDK ne sont plus prises en charge.	7 janvier 2022
Publication initiale	—	30 avril 2021

AWS Glossaire des directives prescriptives

Les termes suivants sont couramment utilisés dans les stratégies, les guides et les modèles fournis par les directives AWS prescriptives. Pour suggérer des entrées, veuillez utiliser le lien Faire un commentaire à la fin du glossaire.

Nombres

7 R

Sept politiques de migration courantes pour transférer des applications vers le cloud. Ces politiques s'appuient sur les 5 R identifiés par Gartner en 2011 et sont les suivantes :

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle dans le. AWS Cloud
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle locale vers Oracle sur une EC2 instance du AWS Cloud.
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers AWS.
- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.

- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue (à l'aide d'un outil de réplication bidirectionnelle ou d'opérations d'écriture double), tandis que les deux bases de données gèrent les transactions provenant de la connexion d'applications pendant la migration. Cette méthode prend en charge la migration par petits lots contrôlés au lieu d'exiger un basculement ponctuel. Elle est plus flexible mais demande plus de travail qu'une migration active-passive.

migration active-passive

Méthode de migration de base de données dans laquelle les bases de données source et cible sont synchronisées, mais seule la base de données source gère les transactions liées à la connexion des applications pendant que les données sont répliquées vers la base de données cible. La base de données cible n'accepte aucune transaction pendant la migration.

fonction d'agrégation

Fonction SQL qui agit sur un groupe de lignes et calcule une valeur de retour unique pour le groupe. Des exemples de fonctions d'agrégation incluent `SUM` et`MAX`.

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

Processus de suppression définitive d'informations personnelles dans un ensemble de données. L'anonymisation peut contribuer à protéger la vie privée. Les données anonymisées ne sont plus considérées comme des données personnelles.

anti-motif

Solution fréquemment utilisée pour un problème récurrent lorsque la solution est contre-productive, inefficace ou moins efficace qu'une alternative.

contrôle des applications

Une approche de sécurité qui permet d'utiliser uniquement des applications approuvées afin de protéger un système contre les logiciels malveillants.

portefeuille d'applications

Ensemble d'informations détaillées sur chaque application utilisée par une organisation, y compris le coût de génération et de maintenance de l'application, ainsi que sa valeur métier. Ces informations sont essentielles pour le processus de découverte et d'analyse du portefeuille et permettent d'identifier et de prioriser les applications à migrer, à moderniser et à optimiser.

intelligence artificielle (IA)

Domaine de l'informatique consacré à l'utilisation des technologies de calcul pour exécuter des fonctions cognitives généralement associées aux humains, telles que l'apprentissage, la résolution de problèmes et la reconnaissance de modèles. Pour plus d'informations, veuillez consulter Qu'est-ce que l'intelligence artificielle ?

opérations d'intelligence artificielle (AIOps)

Processus consistant à utiliser des techniques de machine learning pour résoudre les problèmes opérationnels, réduire les incidents opérationnels et les interventions humaines, mais aussi améliorer la qualité du service. Pour plus d'informations sur son AIOps utilisation dans la stratégie de AWS migration, consultez le guide d'intégration des opérations.

chiffrement asymétrique

Algorithme de chiffrement qui utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Vous pouvez partager la clé publique, car elle n'est pas utilisée pour le déchiffrement, mais l'accès à la clé privée doit être très restreint.

atomicité, cohérence, isolement, durabilité (ACID)

Ensemble de propriétés logicielles garantissant la validité des données et la fiabilité opérationnelle d'une base de données, même en cas d'erreur, de panne de courant ou d'autres problèmes.

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, consultez ABAC pour AWS dans la documentation AWS Identity and Access Management (IAM).

source de données faisant autorité

Emplacement où vous stockez la version principale des données, considérée comme la source d'information la plus fiable. Vous pouvez copier les données de la source de données officielle vers d'autres emplacements à des fins de traitement ou de modification des données, par exemple en les anonymisant, en les expurgant ou en les pseudonymisant.

Zone de disponibilité

Un emplacement distinct au sein d'un Région AWS réseau isolé des défaillances dans d'autres zones de disponibilité et fournissant une connectivité réseau peu coûteuse et à faible latence aux autres zones de disponibilité de la même région.

AWS Cadre d'adoption du cloud (AWS CAF)

Un cadre de directives et de meilleures pratiques visant AWS à aider les entreprises à élaborer un plan efficace pour réussir leur migration vers le cloud. AWS La CAF organise ses conseils en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, la AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications afin de préparer l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

AWS Cadre de qualification de la charge de travail (AWS WQF)

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le WQF est inclus avec

AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

Un bot destiné à perturber ou à nuire à des individus ou à des organisations.

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

Vue unifiée et interactive des comportements des ressources et des interactions au fil du temps. Vous pouvez utiliser un graphique de comportement avec Amazon Detective pour examiner les tentatives de connexion infructueuses, les appels d'API suspects et les actions similaires. Pour plus d'informations, veuillez consulter Data in a behavior graph dans la documentation Detective.

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi endianité.

classification binaire

Processus qui prédit un résultat binaire (l'une des deux classes possibles). Par exemple, votre modèle de machine learning peut avoir besoin de prévoir des problèmes tels que « Cet e-mail est-il du spam ou non ? » ou « Ce produit est-il un livre ou une voiture ? ».

filtre de Bloom

Structure de données probabiliste et efficace en termes de mémoire qui est utilisée pour tester si un élément fait partie d'un ensemble.

déploiement bleu/vert

Stratégie de déploiement dans laquelle vous créez deux environnements distincts mais identiques. Vous exécutez la version actuelle de l'application dans un environnement (bleu) et la nouvelle version de l'application dans l'autre environnement (vert). Cette stratégie vous permet de revenir rapidement en arrière avec un impact minimal.

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, appelés « bots malveillants », sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

Réseaux de robots infectés par des logiciels malveillants et contrôlés par une seule entité, connue sous le nom d'herder ou d'opérateur de bots. Les botnets sont le mécanisme le plus connu pour faire évoluer les bots et leur impact.

branche

Zone contenue d'un référentiel de code. La première branche créée dans un référentiel est la branche principale. Vous pouvez créer une branche à partir d'une branche existante, puis développer des fonctionnalités ou corriger des bogues dans la nouvelle branche. Une branche que vous créez pour générer une fonctionnalité est communément appelée branche de fonctionnalités. Lorsque la fonctionnalité est prête à être publiée, vous fusionnez à nouveau la branche de fonctionnalités dans la branche principale. Pour plus d'informations, consultez À propos des branches (GitHub documentation).

accès par brise-vitre

Dans des circonstances exceptionnelles et par le biais d'un processus approuvé, il s'agit d'un moyen rapide pour un utilisateur d'accéder à un accès auquel Compte AWS il n'est généralement pas autorisé. Pour plus d'informations, consultez l'indicateur Implementation break-glass procedures dans le guide Well-Architected AWS .

stratégie existante (brownfield)

L'infrastructure existante de votre environnement. Lorsque vous adoptez une stratégie existante pour une architecture système, vous concevez l'architecture en fonction des contraintes des systèmes et de l'infrastructure actuels. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

cache de tampon

Zone de mémoire dans laquelle sont stockées les données les plus fréquemment consultées.

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

Plan qui tient compte de l'impact potentiel d'un événement perturbateur, tel qu'une migration à grande échelle, sur les opérations, et qui permet à une entreprise de reprendre ses activités rapidement.

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

Diffusion lente et progressive d'une version pour les utilisateurs finaux. Lorsque vous êtes sûr, vous déployez la nouvelle version et remplacez la version actuelle dans son intégralité.

CCo E

Voir le Centre d'excellence du cloud.

CDC

Consultez la section Capture des données de modification.

capture des données de modification (CDC)

Processus de suivi des modifications apportées à une source de données, telle qu'une table de base de données, et d'enregistrement des métadonnées relatives à ces modifications. Vous pouvez utiliser la CDC à diverses fins, telles que l'audit ou la réplication des modifications dans un système cible afin de maintenir la synchronisation.

ingénierie du chaos

Introduire intentionnellement des défaillances ou des événements perturbateurs pour tester la résilience d'un système. Vous pouvez utiliser AWS Fault Injection Service (AWS FIS) pour effectuer des expériences qui stressent vos AWS charges de travail et évaluer leur réponse.

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

Processus de catégorisation qui permet de générer des prédictions. Les modèles de ML pour les problèmes de classification prédisent une valeur discrète. Les valeurs discrètes se distinguent toujours les unes des autres. Par exemple, un modèle peut avoir besoin d'évaluer la présence ou non d'une voiture sur une image.

chiffrement côté client

Chiffrement des données localement, avant que la cible ne les Service AWS reçoive.

Centre d'excellence du cloud (CCoE)

Une équipe multidisciplinaire qui dirige les efforts d'adoption du cloud au sein d'une organisation, notamment en développant les bonnes pratiques en matière de cloud, en mobilisant des ressources, en établissant des délais de migration et en guidant l'organisation dans le cadre de transformations à grande échelle. Pour plus d'informations, consultez les CCoarticles électroniques du blog sur la stratégie AWS Cloud d'entreprise.

cloud computing

Technologie cloud généralement utilisée pour le stockage de données à distance et la gestion des appareils IoT. Le cloud computing est généralement associé à la technologie informatique de pointe.

modèle d'exploitation du cloud

Dans une organisation informatique, modèle d'exploitation utilisé pour créer, faire évoluer et optimiser un ou plusieurs environnements cloud. Pour plus d'informations, consultez la section Création de votre modèle d'exploitation cloud.

étapes d'adoption du cloud

Les quatre phases que les entreprises traversent généralement lorsqu'elles migrent vers AWS Cloud :

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour accélérer votre adoption du cloud (par exemple, créer une zone de landing zone, définir un CCo E, établir un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

Ces étapes ont été définies par Stephen Orban dans le billet de blog The Journey Toward Cloud-First & the Stages of Adoption publié sur le blog AWS Cloud Enterprise Strategy. Pour plus d'informations sur leur lien avec la stratégie de AWS migration, consultez le guide de préparation à la migration.

CMDB

Consultez la base de données de gestion des configurations.

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub ouBitbucket Cloud. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

cache passif

Cache tampon vide, mal rempli ou contenant des données obsolètes ou non pertinentes. Cela affecte les performances, car l'instance de base de données doit lire à partir de la mémoire principale ou du disque, ce qui est plus lent que la lecture à partir du cache tampon.

données gelées

Données rarement consultées et généralement historiques. Lorsque vous interrogez ce type de données, les requêtes lentes sont généralement acceptables. Le transfert de ces données vers des niveaux ou classes de stockage moins performants et moins coûteux peut réduire les coûts.

vision par ordinateur (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, Amazon SageMaker AI fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

Pour une charge de travail, une modification de configuration par rapport à l'état attendu. Cela peut entraîner une non-conformité de la charge de travail, et cela est généralement progressif et involontaire.

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

Ensemble de AWS Config règles et d'actions correctives que vous pouvez assembler pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans une région Compte AWS et, ou au sein d'une organisation, à l'aide d'un modèle YAML. Pour plus d'informations, consultez la section Packs de conformité dans la AWS Config documentation.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

Données stationnaires dans votre réseau, telles que les données stockées.

classification des données

Processus permettant d'identifier et de catégoriser les données de votre réseau en fonction de leur sévérité et de leur sensibilité. Il s'agit d'un élément essentiel de toute stratégie de gestion des risques de cybersécurité, car il vous aide à déterminer les contrôles de protection et de conservation appropriés pour les données. La classification des données est une composante du pilier de sécurité du AWS Well-Architected Framework. Pour plus d'informations, veuillez consulter Classification des données.

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

Données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau.

maillage de données

Un cadre architectural qui fournit une propriété des données distribuée et décentralisée avec une gestion et une gouvernance centralisées.

minimisation des données

Le principe de collecte et de traitement des seules données strictement nécessaires. La pratique de la minimisation des données AWS Cloud peut réduire les risques liés à la confidentialité, les coûts et l'empreinte carbone de vos analyses.

périmètre de données

Ensemble de garde-fous préventifs dans votre AWS environnement qui permettent de garantir que seules les identités fiables accèdent aux ressources fiables des réseaux attendus. Pour plus d'informations, voir Création d'un périmètre de données sur AWS.

prétraitement des données

Pour transformer les données brutes en un format facile à analyser par votre modèle de ML. Le prétraitement des données peut impliquer la suppression de certaines colonnes ou lignes et le traitement des valeurs manquantes, incohérentes ou en double.

provenance des données

Le processus de suivi de l'origine et de l'historique des données tout au long de leur cycle de vie, par exemple la manière dont les données ont été générées, transmises et stockées.

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

Un système de gestion des données qui prend en charge les informations commerciales, telles que les analyses. Les entrepôts de données contiennent généralement de grandes quantités de données historiques et sont généralement utilisés pour les requêtes et les analyses.

langage de définition de base de données (DDL)

Instructions ou commandes permettant de créer ou de modifier la structure des tables et des objets dans une base de données.

langage de manipulation de base de données (DML)

Instructions ou commandes permettant de modifier (insérer, mettre à jour et supprimer) des informations dans une base de données.

DDL

Voir langage de définition de base de données.

ensemble profond

Sert à combiner plusieurs modèles de deep learning à des fins de prédiction. Vous pouvez utiliser des ensembles profonds pour obtenir une prévision plus précise ou pour estimer l'incertitude des prédictions.

deep learning

Un sous-champ de ML qui utilise plusieurs couches de réseaux neuronaux artificiels pour identifier le mappage entre les données d'entrée et les variables cibles d'intérêt.

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de

la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte AWS membre pour administrer les comptes de l'organisation et gérer les autorisations pour ce service. Ce compte est appelé administrateur délégué pour ce service. Pour plus d'informations et une liste des services compatibles, veuillez consulter la rubrique Services qui fonctionnent avec AWS Organizations dans la documentation AWS Organizations .

déploiement

Processus de mise à disposition d'une application, de nouvelles fonctionnalités ou de corrections de code dans l'environnement cible. Le déploiement implique la mise en œuvre de modifications dans une base de code, puis la génération et l'exécution de cette base de code dans les environnements de l'application.

environnement de développement

Voir environnement.

contrôle de détection

Contrôle de sécurité conçu pour détecter, journaliser et alerter après la survenue d'un événement. Ces contrôles constituent une deuxième ligne de défense et vous alertent en cas d'événements de sécurité qui ont contourné les contrôles préventifs en place. Pour plus d'informations, veuillez consulter la rubrique Contrôles de détection dans Implementing security controls on AWS.

cartographie de la chaîne de valeur du développement (DVSM)

Processus utilisé pour identifier et hiérarchiser les contraintes qui nuisent à la rapidité et à la qualité du cycle de vie du développement logiciel. DVSM étend le processus de cartographie de la chaîne de valeur initialement conçu pour les pratiques de production allégée. Il met l'accent sur les étapes et les équipes nécessaires pour créer et transférer de la valeur tout au long du processus de développement logiciel.

jumeau numérique

Représentation virtuelle d'un système réel, tel qu'un bâtiment, une usine, un équipement industriel ou une ligne de production. Les jumeaux numériques prennent en charge la maintenance prédictive, la surveillance à distance et l'optimisation de la production.

tableau des dimensions

Dans un schéma en étoile, table plus petite contenant les attributs de données relatifs aux données quantitatives d'une table de faits. Les attributs des tables de dimensions sont généralement des champs de texte ou des nombres discrets qui se comportent comme du texte. Ces attributs sont couramment utilisés pour la contrainte des requêtes, le filtrage et l'étiquetage des ensembles de résultats.

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

La stratégie et le processus que vous utilisez pour minimiser les temps d'arrêt et les pertes de données causés par un sinistre. Pour plus d'informations, consultez Disaster Recovery of Workloads on AWS : Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

Approche visant à développer un système logiciel complexe en connectant ses composants à des domaines évolutifs, ou objectifs métier essentiels, que sert chaque composant. Ce concept a été introduit par Eric Evans dans son ouvrage Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur l'utilisation du design piloté par domaine avec le modèle de figuier étrangleur, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

DR

Voir reprise après sinistre.

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour détecter la dérive des ressources du système ou AWS Control Tower

pour détecter les modifications de votre zone d'atterrissage susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

Technologie qui augmente la puissance de calcul des appareils intelligents en périphérie d'un réseau IoT. Comparé au cloud computing, l'informatique de pointe peut réduire la latence des communications et améliorer le temps de réponse.

échange de données informatisé (EDI)

L'échange automatique de documents commerciaux entre les organisations. Pour plus d'informations, voir Qu'est-ce que l'échange de données informatisé ?

chiffrement

Processus informatique qui transforme des données en texte clair, lisibles par l'homme, en texte chiffré.

clé de chiffrement

Chaîne cryptographique de bits aléatoires générée par un algorithme cryptographique. La longueur des clés peut varier, et chaque clé est conçue pour être imprévisible et unique.

endianisme

Ordre selon lequel les octets sont stockés dans la mémoire de l'ordinateur. Les systèmes de poids fort stockent d'abord l'octet le plus significatif. Les systèmes de poids faible stockent d'abord l'octet le moins significatif.

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou à AWS Identity and Access Management (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

planification des ressources d'entreprise (ERP)

Système qui automatise et gère les principaux processus métier (tels que la comptabilité, le MES et la gestion de projet) pour une entreprise.

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, consultez la section Chiffrement des enveloppes dans la documentation AWS Key Management Service (AWS KMS).

environment

Instance d'une application en cours d'exécution. Les types d'environnement les plus courants dans le cloud computing sont les suivants :

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.
- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un CI/CD pipeline, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des

environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

époppée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les points forts de la AWS CAF en matière de sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures, la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS , veuillez consulter le guide d'implémentation du programme.

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

Processus d'analyse d'un jeu de données pour comprendre ses principales caractéristiques. Vous collectez ou agrégez des données, puis vous effectuez des enquêtes initiales pour trouver des modèles, détecter des anomalies et vérifier les hypothèses. L'EDA est réalisée en calculant des statistiques récapitulatives et en créant des visualisations de données.

F

tableau des faits

La table centrale dans un schéma en étoile. Il stocke des données quantitatives sur les opérations commerciales. Généralement, une table de faits contient deux types de colonnes : celles qui contiennent des mesures et celles qui contiennent une clé étrangère pour une table de dimensions.

échouer rapidement

Une philosophie qui utilise des tests fréquents et progressifs pour réduire le cycle de vie du développement. C'est un élément essentiel d'une approche agile.

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des

charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir succursale.

fonctionnalités

Les données d'entrée que vous utilisez pour faire une prédiction. Par exemple, dans un contexte de fabrication, les fonctionnalités peuvent être des images capturées périodiquement à partir de la ligne de fabrication.

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients intégrés. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec AWS.

transformation de fonctionnalité

Optimiser les données pour le processus de ML, notamment en enrichissant les données avec des sources supplémentaires, en mettant à l'échelle les valeurs ou en extrayant plusieurs ensembles d'informations à partir d'un seul champ de données. Cela permet au modèle de ML de tirer parti des données. Par exemple, si vous décomposez la date « 2021-05-27 00:15:37 » en « 2021 », « mai », « jeudi » et « 15 », vous pouvez aider l'algorithme d'apprentissage à apprendre des modèles nuancés associés à différents composants de données.

invitation en quelques coups

Fournir à un LLM un petit nombre d'exemples illustrant la tâche et le résultat souhaité avant de lui demander d'effectuer une tâche similaire. Cette technique est une application de l'apprentissage contextuel, dans le cadre de laquelle les modèles apprennent à partir d'exemples (prises de vue) intégrés dans des instructions. Les instructions en quelques clics peuvent être efficaces pour les tâches qui nécessitent un formatage, un raisonnement ou des connaissances de domaine spécifiques. Voir également l'invite Zero-Shot.

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

Utilisation de plusieurs conditions pour autoriser ou refuser une demande d'accès.

migration instantanée (flash-cut)

Méthode de migration de base de données qui utilise la réplication continue des données par le biais de la capture des données de modification afin de migrer les données dans les plus brefs délais, au lieu d'utiliser une approche progressive. L'objectif est de réduire au maximum les temps d'arrêt.

FM

Voir le modèle de fondation.

modèle de fondation (FM)

Un vaste réseau neuronal d'apprentissage profond qui s'est entraîné sur d'énormes ensembles de données généralisées et non étiquetées. FMs sont capables d'effectuer une grande variété de tâches générales, telles que comprendre le langage, générer du texte et des images et converser en langage naturel. Pour plus d'informations, voir Que sont les modèles de base ?

G

IA générative

Sous-ensemble de modèles d'IA qui ont été entraînés sur de grandes quantités de données et qui peuvent utiliser une simple invite textuelle pour créer de nouveaux contenus et artefacts, tels que des images, des vidéos, du texte et du son. Pour plus d'informations, consultez Qu'est-ce que l'IA générative.

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

Sur Amazon CloudFront, option permettant d'empêcher les utilisateurs de certains pays d'accéder aux distributions de contenu. Vous pouvez utiliser une liste d'autorisation ou une liste de blocage pour spécifier les pays approuvés et interdits. Pour plus d'informations, consultez la section Restreindre la distribution géographique de votre contenu dans la CloudFront documentation.

Flux de travail Gitflow

Approche dans laquelle les environnements inférieurs et supérieurs utilisent différentes branches dans un référentiel de code source. Le flux de travail Gitflow est considéré comme existant, et le flux de travail basé sur les troncs est l'approche moderne préférée.

image dorée

Un instantané d'un système ou d'un logiciel utilisé comme modèle pour déployer de nouvelles instances de ce système ou logiciel. Par exemple, dans le secteur de la fabrication, une image dorée peut être utilisée pour fournir des logiciels sur plusieurs appareils et contribue à améliorer la vitesse, l'évolutivité et la productivité des opérations de fabrication des appareils.

stratégie inédite

L'absence d'infrastructures existantes dans un nouvel environnement. Lorsque vous adoptez une stratégie inédite pour une architecture système, vous pouvez sélectionner toutes les nouvelles technologies sans restriction de compatibilité avec l'infrastructure existante, également appelée brownfield. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités organisationnelles (OUs). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

Migration de votre base de données source vers une base de données cible qui utilise un moteur de base de données différent (par exemple, Oracle vers Amazon Aurora). La migration hétérogène fait généralement partie d'un effort de réarchitecture, et la conversion du schéma peut s'avérer une tâche complexe. AWS propose AWS SCT qui facilite les conversions de schémas.

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation des historiens

Approche utilisée pour moderniser et mettre à niveau les systèmes de technologie opérationnelle (OT) afin de mieux répondre aux besoins de l'industrie manufacturière. Un historien est un type de base de données utilisé pour collecter et stocker des données provenant de diverses sources dans une usine.

données de rétention

Partie de données historiques étiquetées qui n'est pas divulguée dans un ensemble de données utilisé pour entraîner un modèle d'apprentissage automatique. Vous pouvez utiliser les données de blocage pour évaluer les performances du modèle en comparant les prévisions du modèle aux données de blocage.

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données translationnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

correctif

Solution d'urgence à un problème critique dans un environnement de production. En raison de son urgence, un correctif est généralement créé en dehors du flux de travail de DevOps publication habituel.

période de soins intensifs

Immédiatement après le basculement, période pendant laquelle une équipe de migration gère et surveille les applications migrées dans le cloud afin de résoudre les problèmes éventuels. En règle générale, cette période dure de 1 à 4 jours. À la fin de la période de soins intensifs, l'équipe de migration transfère généralement la responsabilité des applications à l'équipe des opérations cloud.

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l’identité

Politique attachée à un ou plusieurs principaux IAM qui définit leurs autorisations au sein de l' AWS Cloud environnement.

application inactive

Application dont l'utilisation moyenne du processeur et de la mémoire se situe entre 5 et 20 % sur une période de 90 jours. Dans un projet de migration, il est courant de retirer ces applications ou de les retenir sur site.

IIo T

Voir Internet industriel des objets.

infrastructure immuable

Modèle qui déploie une nouvelle infrastructure pour les charges de travail de production au lieu de mettre à jour, d'appliquer des correctifs ou de modifier l'infrastructure existante. Les infrastructures immuables sont intrinsèquement plus cohérentes, fiables et prévisibles que les infrastructures mutables. Pour plus d'informations, consultez les meilleures pratiques de déploiement à l'aide d'une infrastructure immuable dans le AWS Well-Architected Framework.

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes

et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

Un terme introduit par Klaus Schwab en 2016 pour désigner la modernisation des processus de fabrication grâce aux avancées en matière de connectivité, de données en temps réel, d'automatisation, d'analyse et d'IA/ML.

infrastructure

Ensemble des ressources et des actifs contenus dans l'environnement d'une application.

infrastructure en tant que code (IaC)

Processus de mise en service et de gestion de l'infrastructure d'une application via un ensemble de fichiers de configuration. IaC est conçue pour vous aider à centraliser la gestion de l'infrastructure, à normaliser les ressources et à mettre à l'échelle rapidement afin que les nouveaux environnements soient reproductibles, fiables et cohérents.

Internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, voir Élaboration d'une stratégie de transformation numérique de l'Internet des objets (IIoT) industriel.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau

avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

Réseau d'objets physiques connectés dotés de capteurs ou de processeurs intégrés qui communiquent avec d'autres appareils et systèmes via Internet ou via un réseau de communication local. Pour plus d'informations, veuillez consulter la section Qu'est-ce que l'IoT ?.

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec AWS.

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. L'ITIL constitue la base de l'ITSM.

gestion des services informatiques (ITSM)

Activités associées à la conception, à la mise en œuvre, à la gestion et à la prise en charge de services informatiques d'une organisation. Pour plus d'informations sur l'intégration des opérations cloud aux outils ITSM, veuillez consulter le guide d'intégration des opérations.

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection

entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu, évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter Setting up a secure and scalable multi-account AWS environment.

grand modèle de langage (LLM)

Un modèle d'intelligence artificielle basé sur le deep learning qui est préentraîné sur une grande quantité de données. Un LLM peut effectuer plusieurs tâches, telles que répondre à des questions, résumer des documents, traduire du texte dans d'autres langues et compléter des phrases. Pour plus d'informations, voir Que sont LLMs.

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

Bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour plus d'informations, veuillez consulter la rubrique Accorder les autorisations de moindre privilège dans la documentation IAM.

lift and shift

Voir 7 Rs.

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi endianité.

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

Type d'intelligence artificielle qui utilise des algorithmes et des techniques pour la reconnaissance et l'apprentissage de modèles. Le ML analyse et apprend à partir de données enregistrées, telles que les données de l'Internet des objets (IoT), pour générer un modèle statistique basé sur des modèles. Pour plus d'informations, veuillez consulter Machine Learning.

branche principale

Voir succursale.

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

Services AWS pour lequel AWS fonctionnent la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données. Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB sont des exemples de services gérés. Ils sont également appelés services abstraits.

système d'exécution de la fabrication (MES)

Un système logiciel pour le suivi, la surveillance, la documentation et le contrôle des processus de production qui convertissent les matières premières en produits finis dans l'atelier.

MAP

Voir Migration Acceleration Program.

mécanisme

Processus complet au cours duquel vous créez un outil, favorisez son adoption, puis inspectez les résultats afin de procéder aux ajustements nécessaires. Un mécanisme est un cycle qui se renforce et s'améliore lorsqu'il fonctionne. Pour plus d'informations, voir Création de mécanismes dans le cadre AWS Well-Architected.

compte membre

Tous, à l' Comptes AWS exception du compte de gestion, qui font partie d'une organisation dans AWS Organizations. Un compte ne peut être membre que d'une seule organisation à la fois.

MAILLES

Voir le système d'exécution de la fabrication.

Transport télémétrique en file d'attente de messages (MQTT)

Protocole de communication léger machine-to-machine (M2M), basé sur le modèle de publication/d'abonnement, pour les appareils IoT aux ressources limitées.

microservice

Un petit service indépendant qui communique via un réseau bien défini APIs et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section Intégration de microservices à l'aide de services AWS sans serveur.

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie en utilisant Lightweight. APIs Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, consultez la section Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

Un AWS programme qui fournit un support de conseil, des formations et des services pour aider les entreprises à établir une base opérationnelle solide pour passer au cloud, et pour aider à compenser le coût initial des migrations. MAP inclut une méthodologie de migration pour exécuter les migrations héritées de manière méthodique, ainsi qu'un ensemble d'outils pour automatiser et accélérer les scénarios de migration courants.

migration à grande échelle

Processus consistant à transférer la majeure partie du portefeuille d'applications vers le cloud par vagues, un plus grand nombre d'applications étant déplacées plus rapidement à chaque vague. Cette phase utilise les bonnes pratiques et les enseignements tirés des phases précédentes pour implémenter une usine de migration d'équipes, d'outils et de processus en vue de rationaliser la migration des charges de travail grâce à l'automatisation et à la livraison agile. Il s'agit de la troisième phase de la stratégie de migration AWS.

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des professionnels travaillant dans le cadre de sprints. Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration. Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le AWS compte.

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réorganisez la migration vers Amazon EC2 avec le service de migration AWS d'applications.

Évaluation du portefeuille de migration (MPA)

Outil en ligne qui fournit des informations pour valider l'analyse de rentabilisation en faveur de la migration vers le. AWS Cloud La MPA propose une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, comparaison du coût total de possession, analyse des coûts de migration), ainsi que la planification de la migration (analyse et collecte des données d'applications, regroupement des applications, priorisation des migrations et planification des vagues). L'outil MPA (connexion requise) est disponible gratuitement pour tous les AWS consultants et consultants APN Partner.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une organisation au cloud, à identifier les forces et les faiblesses et à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide du AWS CAF. Pour plus d'informations, veuillez consulter le guide de préparation à la migration. La MRA est la première phase de la stratégie de migration AWS.

stratégie de migration

L'approche utilisée pour migrer une charge de travail vers le AWS Cloud. Pour plus d'informations, reportez-vous aux 7 R de ce glossaire et à Mobiliser votre organisation pour accélérer les migrations à grande échelle.

ML

Voir apprentissage automatique.

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, consultez la section Stratégie de modernisation des applications dans le AWS Cloud.

évaluation de la préparation à la modernisation

Évaluation qui permet de déterminer si les applications d'une organisation sont prêtes à être modernisées, d'identifier les avantages, les risques et les dépendances, et qui détermine dans quelle mesure l'organisation peut prendre en charge l'état futur de ces applications. Le résultat de l'évaluation est un plan de l'architecture cible, une feuille de route détaillant les phases de développement et les étapes du processus de modernisation, ainsi qu'un plan d'action pour combler les lacunes identifiées. Pour plus d'informations, consultez la section Évaluation de l'état de préparation à la modernisation des applications dans le AWS Cloud.

applications monolithiques (monolithes)

Applications qui s'exécutent en tant que service unique avec des processus étroitement couplés. Les applications monolithiques ont plusieurs inconvénients. Si une fonctionnalité de l'application connaît un pic de demande, l'architecture entière doit être mise à l'échelle. L'ajout ou l'amélioration des fonctionnalités d'une application monolithique devient également plus complexe lorsque la base de code s'élargit. Pour résoudre ces problèmes, vous pouvez utiliser une architecture de microservices. Pour plus d'informations, veuillez consulter Decomposing monoliths into microservices.

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

Processus qui permet de générer des prédictions pour plusieurs classes (prédiction d'un résultat parmi plus de deux). Par exemple, un modèle de ML peut demander « Ce produit est-il un livre, une voiture ou un téléphone ? » ou « Quelle catégorie de produits intéresse le plus ce client ? ».

infrastructure mutable

Modèle qui met à jour et modifie l'infrastructure existante pour les charges de travail de production. Pour améliorer la cohérence, la fiabilité et la prévisibilité, le AWS Well-Architected Framework recommande l'utilisation d'une infrastructure immuable comme meilleure pratique.

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

Méthode de migration dans laquelle la charge de travail source est supprimée au cours du processus de migration. Cette méthode implique un temps d'arrêt prolongé et est généralement utilisée pour de petites charges de travail non critiques.

OI

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

Méthode de migration dans laquelle la charge de travail source est copiée sur le système cible sans être mise hors ligne. Les applications connectées à la charge de travail peuvent continuer à fonctionner pendant la migration. Cette méthode implique un temps d'arrêt nul ou minimal et est généralement utilisée pour les charges de travail de production critiques.

OPC-UA

Voir Open Process Communications - Architecture unifiée.

Communications par processus ouvert - Architecture unifiée (OPC-UA)

Un protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle. L'OPC-UA fournit une norme d'interopérabilité avec des schémas de cryptage, d'authentification et d'autorisation des données.

accord au niveau opérationnel (OLA)

Accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de prendre en charge un contrat de niveau de service (SLA).

examen de l'état de préparation opérationnelle (ORR)

Une liste de questions et de bonnes pratiques associées qui vous aident à comprendre, à évaluer, à prévenir ou à réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

technologie opérationnelle (OT)

Systèmes matériels et logiciels qui fonctionnent avec l'environnement physique pour contrôler les opérations, les équipements et les infrastructures industriels. Dans le secteur manufacturier, l'intégration des systèmes OT et des technologies de l'information (IT) est au cœur des transformations de l'industrie 4.0.

intégration des opérations (OI)

Processus de modernisation des opérations dans le cloud, qui implique la planification de la préparation, l'automatisation et l'intégration. Pour en savoir plus, veuillez consulter le guide d'intégration des opérations.

journal de suivi d'organisation

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre est appelé accélération du personnel, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

Dans CloudFront, une option améliorée pour restreindre l'accès afin de sécuriser votre contenu Amazon Simple Storage Service (Amazon S3). L'OAC prend en charge tous les compartiments S3 dans leur ensemble Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les requêtes dynamiques `PUT` adressées au compartiment S3. `DELETE`

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés ne peuvent accéder au contenu d'un compartiment S3 que par le biais d'une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus précis et amélioré.

ORR

Voir l'examen de l'état de préparation opérationnelle.

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS multi-comptes, un VPC qui gère les connexions réseau initiées depuis une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

P

limite des autorisations

Politique de gestion IAM attachée aux principaux IAM pour définir les autorisations maximales que peut avoir l'utilisateur ou le rôle. Pour plus d'informations, veuillez consulter la rubrique Limites des autorisations dans la documentation IAM.

informations personnelles identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. Les exemples d'informations personnelles incluent les noms, les adresses et les coordonnées.

PII

Voir les informations personnelles identifiables.

manuel stratégique

Ensemble d'étapes prédéfinies qui capturent le travail associé aux migrations, comme la fourniture de fonctions d'opérations de base dans le cloud. Un manuel stratégique peut revêtir la forme de scripts, de runbooks automatisés ou d'un résumé des processus ou des étapes nécessaires au fonctionnement de votre environnement modernisé.

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

Objet capable de définir les autorisations (voir la politique basée sur l'identité), de spécifier les conditions d'accès (voir la politique basée sur les ressources) ou de définir les autorisations

maximales pour tous les comptes d'une organisation dans AWS Organizations (voir la politique de contrôle des services).

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

évaluation du portefeuille

Processus de découverte, d'analyse et de priorisation du portefeuille d'applications afin de planifier la migration. Pour plus d'informations, veuillez consulter Evaluating migration readiness.

predicate

Une condition de requête qui renvoie `true` ou`false`, généralement située dans une `WHERE` clause.

prédicat pushdown

Technique d'optimisation des requêtes de base de données qui filtre les données de la requête avant le transfert. Cela réduit la quantité de données qui doivent être extraites et traitées à partir de la base de données relationnelle et améliore les performances des requêtes.

contrôle préventif

Contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Ces contrôles constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute modification indésirable de votre réseau. Pour plus d'informations, veuillez consulter Preventative controls dans Implementing security controls on AWS.

principal

Entité AWS capable d'effectuer des actions et d'accéder aux ressources. Cette entité est généralement un utilisateur root pour un Compte AWS rôle IAM ou un utilisateur. Pour plus d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

confidentialité dès la conception

Une approche d'ingénierie système qui prend en compte la confidentialité tout au long du processus de développement.

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs VPCs domaines. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

gestion du cycle de vie des produits (PLM)

Gestion des données et des processus d'un produit tout au long de son cycle de vie, depuis la conception, le développement et le lancement, en passant par la croissance et la maturité, jusqu'au déclin et au retrait.

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

Dans le secteur manufacturier, un ordinateur hautement fiable et adaptable qui surveille les machines et automatise les processus de fabrication.

chaînage rapide

Utiliser le résultat d'une invite LLM comme entrée pour l'invite suivante afin de générer de meilleures réponses. Cette technique est utilisée pour décomposer une tâche complexe en sous-tâches ou pour affiner ou développer de manière itérative une réponse préliminaire. Cela permet d'améliorer la précision et la pertinence des réponses d'un modèle et permet d'obtenir des résultats plus précis et personnalisés.

pseudonymisation

Processus de remplacement des identifiants personnels dans un ensemble de données par des valeurs fictives. La pseudonymisation peut contribuer à protéger la vie privée. Les données pseudonymisées sont toujours considérées comme des données personnelles.

publish/subscribe (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

Série d'étapes, telles que des instructions, utilisées pour accéder aux données d'un système de base de données relationnelle SQL.

régression du plan de requêtes

Le cas où un optimiseur de service de base de données choisit un plan moins optimal qu'avant une modification donnée de l'environnement de base de données. Cela peut être dû à des changements en termes de statistiques, de contraintes, de paramètres d'environnement, de liaisons de paramètres de requêtes et de mises à jour du moteur de base de données.

R

Matrice RACI

Voir responsable, responsable, consulté, informé (RACI).

CHIFFON

Voir Retrieval Augmented Generation.

rançongiciel

Logiciel malveillant conçu pour bloquer l'accès à un système informatique ou à des données jusqu'à ce qu'un paiement soit effectué.

Matrice RASCI

Voir responsable, responsable, consulté, informé (RACI).

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

Copie d'une base de données utilisée en lecture seule. Vous pouvez acheminer les requêtes vers le réplica de lecture pour réduire la charge sur votre base de données principale.

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise et l'interruption du service.

objectif de temps de récupération (RTO)

Le délai maximum acceptable entre l'interruption du service et le rétablissement du service.

refactoriser

Voir 7 Rs.

Région

Ensemble de AWS ressources dans une zone géographique. Chacun Région AWS est isolé et indépendant des autres pour garantir tolérance aux pannes, stabilité et résilience. Pour plus d'informations, voir Spécifier ce que Régions AWS votre compte peut utiliser.

régression

Technique de ML qui prédit une valeur numérique. Par exemple, pour résoudre le problème « Quel sera le prix de vente de cette maison ? », un modèle de ML pourrait utiliser un modèle de régression linéaire pour prédire le prix de vente d'une maison sur la base de faits connus à son sujet (par exemple, la superficie en mètres carrés).

réhéberger

Voir 7 Rs.

version

Dans un processus de déploiement, action visant à promouvoir les modifications apportées à un environnement de production.

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

La capacité d'une application à résister aux perturbations ou à s'en remettre. La haute disponibilité et la reprise après sinistre sont des considérations courantes lors de la planification de la résilience dans le AWS Cloud. Pour plus d'informations, consultez AWS Cloud Résilience.

politique basée sur les ressources

Politique attachée à une ressource, comme un compartiment Amazon S3, un point de terminaison ou une clé de chiffrement. Ce type de politique précise les principaux auxquels l'accès est autorisé, les actions prises en charge et toutes les autres conditions qui doivent être remplies.

matrice responsable, redevable, consulté et informé (RACI)

Une matrice qui définit les rôles et les responsabilités de toutes les parties impliquées dans les activités de migration et les opérations cloud. Le nom de la matrice est dérivé des types de responsabilité définis dans la matrice : responsable (R), responsable (A), consulté (C) et informé (I). Le type de support (S) est facultatif. Si vous incluez le support, la matrice est appelée matrice RASCI, et si vous l'excluez, elle est appelée matrice RACI.

contrôle réactif

Contrôle de sécurité conçu pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence de sécurité. Pour plus d'informations, veuillez consulter la rubrique Responsive controls dans Implementing security controls on AWS.

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération (RAG)

Technologie d'IA générative dans laquelle un LLM fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir Qu'est-ce que RAG ?

rotation

Processus de mise à jour périodique d'un secret pour empêcher un attaquant d'accéder aux informations d'identification.

contrôle d'accès aux lignes et aux colonnes (RCAC)

Utilisation d'expressions SQL simples et flexibles dotées de règles d'accès définies. Le RCAC comprend des autorisations de ligne et des masques de colonnes.

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de temps de rétablissement.

runbook

Ensemble de procédures manuelles ou automatisées nécessaires à l'exécution d'une tâche spécifique. Elles visent généralement à rationaliser les opérations ou les procédures répétitives présentant des taux d'erreur élevés.

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter

AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

Dans AWS Secrets Manager des informations confidentielles ou restreintes, telles qu'un mot de passe ou des informations d'identification utilisateur, que vous stockez sous forme cryptée. Il comprend la valeur secrète et ses métadonnées. La valeur secrète peut être binaire, une chaîne unique ou plusieurs chaînes. Pour plus d'informations, voir Que contient le secret d'un Secrets Manager ? dans la documentation de Secrets Manager.

sécurité dès la conception

Une approche d'ingénierie système qui prend en compte la sécurité tout au long du processus de développement.

contrôle de sécurité

Barrière de protection technique ou administrative qui empêche, détecte ou réduit la capacité d'un assaillant d'exploiter une vulnérabilité de sécurité. Il existe quatre principaux types de contrôles de sécurité : préventifs, détectifs, réactifs et proactifs.

renforcement de la sécurité

Processus qui consiste à réduire la surface d'attaque pour la rendre plus résistante aux attaques. Cela peut inclure des actions telles que la suppression de ressources qui ne sont plus requises, la mise en œuvre des bonnes pratiques de sécurité consistant à accorder le moindre privilège ou la désactivation de fonctionnalités inutiles dans les fichiers de configuration.

système de gestion des informations et des événements de sécurité (SIEM)

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les

données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs qui vous aident à mettre en œuvre les meilleures pratiques AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une EC2 instance Amazon ou la rotation des informations d'identification.

chiffrement côté serveur

Chiffrement des données à destination, par celui Service AWS qui les reçoit.

Politique de contrôle des services (SCP)

Politique qui fournit un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPs définissez des garde-fous ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez les utiliser SCPs comme listes d'autorisation ou de refus pour spécifier les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

point de terminaison du service

URL du point d'entrée pour un Service AWS. Pour vous connecter par programmation au service cible, vous pouvez utiliser un point de terminaison. Pour plus d'informations, veuillez consulter la rubrique Service AWS endpoints dans Références générales AWS.

contrat de niveau de service (SLA)

Accord qui précise ce qu'une équipe informatique promet de fournir à ses clients, comme le temps de disponibilité et les performances des services.

indicateur de niveau de service (SLI)

Mesure d'un aspect des performances d'un service, tel que son taux d'erreur, sa disponibilité ou son débit.

objectif de niveau de service (SLO)

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de niveau de service.

modèle de responsabilité partagée

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWS est responsable de la sécurité du cloud, alors que vous êtes responsable de la sécurité dans le cloud. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.

SIEM

Consultez les informations de sécurité et le système de gestion des événements.

point de défaillance unique (SPOF)

Défaillance d'un seul composant critique d'une application susceptible de perturber le système.

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

Modèle permettant de mettre à l'échelle et d'accélérer les projets de modernisation. Au fur et à mesure que les nouvelles fonctionnalités et les nouvelles versions de produits sont définies, l'équipe principale se divise pour créer des équipes de produit. Cela permet de mettre à l'échelle les capacités et les services de votre organisation, d'améliorer la productivité des développeurs et de favoriser une innovation rapide. Pour plus d'informations, consultez la section Approche progressive de la modernisation des applications dans le. AWS Cloud

SPOF

Voir point de défaillance unique.

schéma en étoile

Structure organisationnelle de base de données qui utilise une grande table de faits pour stocker les données transactionnelles ou mesurées et utilise une ou plusieurs tables dimensionnelles plus petites pour stocker les attributs des données. Cette structure est conçue pour être utilisée dans un entrepôt de données ou à des fins de business intelligence.

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

Plage d'adresses IP dans votre VPC. Un sous-réseau doit se trouver dans une seule zone de disponibilité.

contrôle de supervision et acquisition de données (SCADA)

Dans le secteur manufacturier, un système qui utilise du matériel et des logiciels pour surveiller les actifs physiques et les opérations de production.

chiffrement symétrique

Algorithme de chiffrement qui utilise la même clé pour chiffrer et déchiffrer les données.

tests synthétiques

Tester un système de manière à simuler les interactions des utilisateurs afin de détecter les problèmes potentiels ou de surveiller les performances. Vous pouvez utiliser Amazon CloudWatch Synthetics pour créer ces tests.

invite du système

Technique permettant de fournir un contexte, des instructions ou des directives à un LLM afin d'orienter son comportement. Les instructions du système aident à définir le contexte et à établir des règles pour les interactions avec les utilisateurs.

T

balises

Des paires clé-valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources. Pour plus d'informations, veuillez consulter la rubrique Balisage de vos AWS ressources.

variable cible

La valeur que vous essayez de prédire dans le cadre du ML supervisé. Elle est également qualifiée de variable de résultat. Par exemple, dans un environnement de fabrication, la variable cible peut être un défaut du produit.

liste de tâches

Outil utilisé pour suivre les progrès dans un runbook. Liste de tâches qui contient une vue d'ensemble du runbook et une liste des tâches générales à effectuer. Pour chaque tâche générale, elle inclut le temps estimé nécessaire, le propriétaire et l'avancement.

environnement de test

Voir environnement.

entraînement

Pour fournir des données à partir desquelles votre modèle de ML peut apprendre. Les données d'entraînement doivent contenir la bonne réponse. L'algorithme d'apprentissage identifie des modèles dans les données d'entraînement, qui mettent en correspondance les attributs des données d'entrée avec la cible (la réponse que vous souhaitez prédire). Il fournit un modèle de ML qui capture ces modèles. Vous pouvez alors utiliser le modèle de ML pour obtenir des prédictions sur de nouvelles données pour lesquelles vous ne connaissez pas la cible.

passerelle de transit

Un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Pour plus d'informations, voir Qu'est-ce qu'une passerelle de transit dans la AWS Transit Gateway documentation.

flux de travail basé sur jonction

Approche selon laquelle les développeurs génèrent et testent des fonctionnalités localement dans une branche de fonctionnalités, puis fusionnent ces modifications dans la branche principale. La branche principale est ensuite intégrée aux environnements de développement, de préproduction et de production, de manière séquentielle.

accès sécurisé

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation AWS Organizations et dans ses comptes en votre nom. Le service de

confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

réglage

Pour modifier certains aspects de votre processus d'entraînement afin d'améliorer la précision du modèle de ML. Par exemple, vous pouvez entraîner le modèle de ML en générant un ensemble d'étiquetage, en ajoutant des étiquettes, puis en répétant ces étapes plusieurs fois avec différents paramètres pour optimiser le modèle.

équipe de deux pizzas

Une petite DevOps équipe que vous pouvez nourrir avec deux pizzas. Une équipe de deux pizzas garantit les meilleures opportunités de collaboration possible dans le développement de logiciels.

U

incertitude

Un concept qui fait référence à des informations imprécises, incomplètes ou inconnues susceptibles de compromettre la fiabilité des modèles de ML prédictifs. Il existe deux types d'incertitude : l'incertitude épistémique est causée par des données limitées et incomplètes, alors que l'incertitude aléatoire est causée par le bruit et le caractère aléatoire inhérents aux données. Pour plus d'informations, veuillez consulter le guide Quantifying uncertainty in deep learning systems.

tâches indifférenciées

Également connu sous le nom de « levage de charges lourdes », ce travail est nécessaire pour créer et exploiter une application, mais qui n'apporte pas de valeur directe à l'utilisateur final ni d'avantage concurrentiel. Les exemples de tâches indifférenciées incluent l'approvisionnement, la maintenance et la planification des capacités.

environnements supérieurs

Voir environnement.

V

mise à vide

Opération de maintenance de base de données qui implique un nettoyage après des mises à jour incrémentielles afin de récupérer de l'espace de stockage et d'améliorer les performances.

contrôle de version

Processus et outils permettant de suivre les modifications, telles que les modifications apportées au code source dans un référentiel.

Appairage de VPC

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC ? dans la documentation Amazon VPC.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

Cache tampon qui contient les données actuelles et pertinentes fréquemment consultées. L'instance de base de données peut lire à partir du cache tampon, ce qui est plus rapide que la lecture à partir de la mémoire principale ou du disque.

données chaudes

Données rarement consultées. Lorsque vous interrogez ce type de données, des requêtes modérément lentes sont généralement acceptables.

fonction de fenêtre

Fonction SQL qui effectue un calcul sur un groupe de lignes liées d'une manière ou d'une autre à l'enregistrement en cours. Les fonctions de fenêtre sont utiles pour traiter des tâches, telles que le calcul d'une moyenne mobile ou l'accès à la valeur des lignes en fonction de la position relative de la ligne en cours.

charge de travail

Ensemble de ressources et de code qui fournit une valeur métier, par exemple une application destinée au client ou un processus de backend.

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet. Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir écrire une fois, lire plusieurs.

WQF

Voir le cadre AWS de qualification de la charge de travail.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire, mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

Une attaque, généralement un logiciel malveillant, qui tire parti d'une vulnérabilité de type « jour zéro ».

vulnérabilité « jour zéro »

Une faille ou une vulnérabilité non atténuée dans un système de production. Les acteurs malveillants peuvent utiliser ce type de vulnérabilité pour attaquer le système. Les développeurs prennent souvent conscience de la vulnérabilité à la suite de l'attaque.

invite Zero-Shot

Fournir à un LLM des instructions pour effectuer une tâche, mais aucun exemple (plans) pouvant aider à la guider. Le LLM doit utiliser ses connaissances pré-entraînées pour gérer la tâche. L'efficacité de l'invite zéro dépend de la complexité de la tâche et de la qualité de l'invite. Voir également les instructions en quelques clics.

application zombie

Application dont l'utilisation moyenne du processeur et de la mémoire est inférieure à 5 %. Dans un projet de migration, il est courant de retirer ces applications.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.