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 CloudWatch et la surveillance avec Amazon et les services de gestion et de gouvernance Amazon Web Services (AWS) associés 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 locaux. AWS Lambda Le guide est destiné aux équipes opérationnelles, aux DevOps ingénieurs et aux ingénieurs d'applications qui gèrent les charges de travail sur leAWS cloud.

Votre approche de journalisation et de surveillance doit être basée sur les six piliers duAWS 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 de manière proactive votre infrastructure.

Ce guide ne traite pas de manière approfondie 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 nombreuxAWS 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. Vous pouvez également utiliser AWS Cost Explorerles AWSbudgets et les indicateursCloudWatch de facturation pour optimiser les coûts.

Le tableau suivant décrit les six domaines que votre solution de journalisation et de surveillance doit prendre en compte.

Capture et ingestion de fichiers journaux et de mesures	Identifiez, configurez et envoyez des journaux et des métriques du système et des applicati ons àAWS des services provenant de différent es 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.
Mesures 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 des applications dans les systèmes et les dépendances externes pour affiner les performances, effectuer une analyse des causes profondes et résoudre les problèmes.
Création de tableaux de bord et de visualisations	Créez des tableaux de bord qui se concentrent sur les mesures et les observations pertinentes pour vos systèmes et vos charges de travail, ce qui favorise l'amélioration continue et 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 nombreuxAWS services fournissent automatiquement des CloudWatch mesures, 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 (à la fois dans le cloud et sur site), les conteneurs et l'informatique sans serveur. Ce guide couvre également lesAWS services suivants utilisés pour la journalisation et la surveillance :

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

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

Les services deAWS calcul 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 l'implémentation et la configuration de Amazon EC2, Amazon ECS, Amazon EKS et Lambda sont différentes.

Les propriétaires d'applications et de 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 prendre en compte la couche systèmes pour les journaux et les mesures au niveau du système d'exploitation (OS), en plus de la couche application pour les journaux et les mesures des applications. Le guide propose une approche recommandée pour traiter ces deux couches selon différents types de calcul, y compris les trois types de calcul décrits dans le tableau suivant.

Instances EC2 immuables et de longue durée	Journaux et mesures des systèmes et des applications sur plusieurs systèmes d'exploit ation (OS) dans plusieursAWS 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 aborde CloudWatch et fournitAWS des services connexes dans les domaines suivants :

- Planification de votre CloudWatch déploiement— Considérations relatives à la planification de votre CloudWatch déploiement et conseils pour centraliser votre CloudWatch configuration.
- Configuration de CloudWatch agent pour instances EC2 et serveurs sur site— détails CloudWatch de configuration pour la journalisation et les métriques au niveau du système et de l'application.
- Approches d'installation de l'agent CloudWatch pour Amazon EC2 et les serveurs locaux— Approches d'installation de l' CloudWatch agent, y compris le déploiement automatique à l'aide de Systems Manager dans plusieurs régions et comptes.
- Journalisation et surveillance sur Amazon ECS — Conseils CloudWatch pour la configuration de la journalisation et des métriques au niveau du cluster et de l'application dans Amazon ECS.
- Journalisation et surveillance sur Amazon EKS — Conseils CloudWatch pour la configuration de la journalisation et des métriques au niveau du cluster et de l'application dans Amazon EKS.
- Surveillance Prometheus sur Amazon EKS— Présente et compare Amazon Managed Service pour Prometheus avec la surveillance CloudWatch Container Insights pour Prometheus.
- Journalisation et statistiques pourAWS Lambda— Conseils CloudWatch pour la configuration de vos fonctions Lambda.
- Recherche et analyse des connexions CloudWatch— Méthodes pour analyser vos journaux à l'aide d'Amazon CloudWatch Application Insights, de CloudWatch Logs Insights et d'extension de l'analyse des journaux à Amazon OpenSearch Service.
- Des options alarmantes avec CloudWatch— Présente la détection des CloudWatch alarmes et 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 contrôles de santé de CloudWatch Synthetics et de Route 53 pour une surveillance automatique de la disponibilité.
- Tracer les applications avecAWS 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 desAWS charges de travail.
- Intégration de CloudWatch àAWSservices— Explique comment CloudWatch s'intègre à diversAWS services.
- Amazon Managed Grafana pour le tableau de bord et la visualisation— Présente et compare Amazon Managed Grafana à des CloudWatch fins de tableau de bord et de visualisation.

Des exemples d'implémentation sont utilisés tout au long de ce guide dans ces domaines et sont également disponibles dans le GitHub référentielAWS d'échantillons.

Résultats commerciaux ciblés

Création d'une solution de journalisation et de surveillance conçue pour leAWSLe cloud fait partie intégrante de la réalisation dusix avantages du cloud computing. Votre solution de journalisation et de surveillance doit aider votre organisation informatique à atteindre des résultats commerciaux qui profitent à vos processus commerciaux, à vos partenaires commerciaux, à vos employés et à vos clients. Vous pouvez vous attendre aux quatre résultats suivants après avoir implémenté une solution de journalisation et de surveillance alignée sur leAWSFramework Well-Architected :

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 goulot d'étranglement si vous comptez trop sur des processus manuels et peut également réduire le temps de valorisation (TTV) pour vos investissements informatiques. Une approche inefficace entraîne également 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 métier.

Vous pouvez utiliser les approches de ce guide pour normaliser et automatiser votre journalisation et votre surveillance sur leAWScloud. Les nouvelles charges de travail nécessitent ensuite une préparation et une intervention manuelles minimales pour la journalisation et la surveillance de la production. Cela permet également de réduire le temps et les étapes nécessaires à la création de normes de journalisation et de surveillance à grande échelle pour différentes charges de travail sur plusieurs comptes et régions.

Améliorer l'excellence opérationnelle

Ce guide fournit plusieurs bonnes pratiques pour la journalisation et la surveillance qui aident diverses charges de travail à atteindre les objectifs de l'entreprise etExcellence opérationnelle. Ce guide fournit égalementexemples détaillés et modèles open source réutilisablesque vous pouvez utiliser avec une approche d'infrastructure en tant que code (iAC) pour implémenter une solution de journalisation et de surveillance bien architecturée à l'aideAWSServices . L'amélioration de l'excellence opérationnelle est itérative et nécessite une amélioration continue. Le guide fournit des suggestions sur la façon d'améliorer continuellement les pratiques de journalisation et de surveillance.

Améliorez la visibilité opérationnelle

Vos processus métiers et applications peuvent être pris en charge par différentes ressources informatiques et hébergés sur différents types de calcul, que ce soit sur site ou sur leAWScloud. Votre visibilité opérationnelle peut être limitée par des implémentations incohérentes et incomplètes de votre stratégie de journalisation et de surveillance. L'adoption d'une approche complète de journalisation et de surveillance vous aide à identifier, diagnostiquer et réagir rapidement aux 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 des défaillances (MTTR). Une approche complète de journalisation et de surveillance aide également votre organisation à améliorer la qualité du service, à améliorer l'expérience de l'utilisateur final et à respecter les accords de niveau de service (SLA).

Faites évoluer les opérations et réduire les frais généraux

Vous pouvez faire évoluer les pratiques de journalisation et de surveillance à partir de ce guide pour prendre en charge plusieurs régions et comptes, des ressources de courte durée et plusieurs environnements. Le guide fournit des approches et des exemples permettant d'automatiser les étapes manuelles (par exemple, installer et configurer des agents, surveiller les mesures, notifier ou prendre des mesures lorsque des problèmes surviennent). Ces approches sont utiles lorsque votre adoption du cloud arrive à maturité et augmente et que vous devez faire évoluer la capacité opérationnelle 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 les systèmes d'exploitation 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 de déploiement et de configuration.

Nous vous recommandons CloudWatch de l'utiliser pour capturer et ingérer des journaux et des métriques pour plusieurs systèmes d'exploitation et 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 systèmes d'exploitation et 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 à des fins de sécurité, d'archivage, de surveillance et d'analyse.
Exigences 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 SDK AWS pour écrire votre propre application de traitement personnalisée dans la langue de votre choix, lire les journaux et les statistiques 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 tous 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' CloudWatchagent 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 sous forme de paramètres de magasin de paramètres ou de 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 instances EC2 en une seule fois. 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'instances EC2 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'instances EC2 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 configurations standard d'Amazon EC2 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 ou AWS CodeCommit) 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 entre vos comptes et régions.

Configuration de CloudWatch agent pour instances EC2 et serveurs sur site

De nombreuses organisations exécutent des charges de travail sur des serveurs physiques et des machines virtuelles (VM). Ces charges de travail s'exécutent généralement sur différents systèmes d'exploitation qui ont chacun des exigences d'installation et de configuration uniques pour la capture et l'ingestion de mesures.

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

Organizations qui migrent ou étendent leurs investissements informatiques vers leAWSLe cloud peut tirer parti CloudWatch pour obtenir une solution unifiée de journalisation et de surveillance. CloudWatch la tarification signifie que vous payez progressivement les mesures et les journaux que vous souhaitez capturer. Vous pouvez également capturer des journaux et des mesures pour des serveurs locaux à l'aide d'un outil similaire CloudWatch processus d'installation de l'agent comme celui d'Amazon EC2.

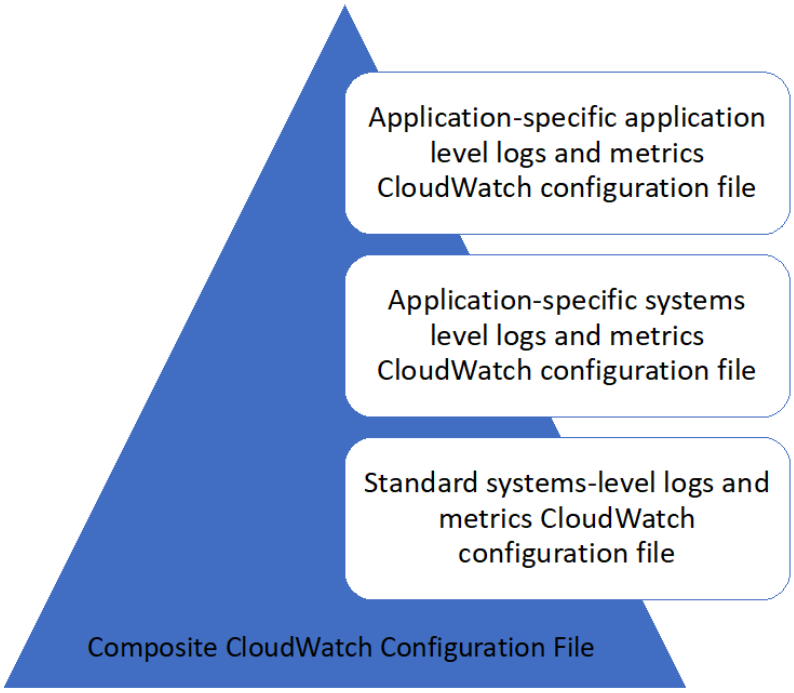
Avant de commencer à installer et à déployer CloudWatch, assurez-vous d'évaluer les configurations de journalisation et de mesure de vos systèmes et applications. Assurez-vous de définir les journaux et les mesures standard que vous devez capturer pour les systèmes d'exploitation que vous souhaitez utiliser. Les journaux et les mesures 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 mesures et des fichiers journaux importants sont disponibles dans les distributions Linux, en plus de celles spécifiques à une version ou à une distribution Linux. Cette variance se produit également entre les différentes versions de Windows.

Configuration de CloudWatch agent

CloudWatch capture les métriques et les journaux pour Amazon EC2 et les serveurs sur site à l'aide deAgents CloudWatch et fichiers de configuration des agentsqui sont propres à chaque système

d'exploitation. Nous vous recommandons de définir la configuration standard de mesure et de capture de journaux de votre organisation avant de commencer à installer le CloudWatch agent à grande échelle dans vos comptes.

Vous pouvez combiner plusieurs CloudWatch configurations d'agent pour former un composite CloudWatch configuration de l'agent. Une approche recommandée consiste à définir et à diviser les configurations de vos journaux et mesures au niveau du système et de l'application. Le diagramme suivant illustre comment plusieurs types de fichiers de configuration CloudWatch pour différentes exigences peuvent être combinés pour former une configuration CloudWatch composite :



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

Configuration de la capture de journaux pour les instances EC2

Par défaut, Amazon EC2 ne surveille ni ne capture de fichiers journaux. Au lieu de cela, les fichiers journaux sont capturés et ingérés dans CloudWatch Journaux par le CloudWatch logiciel d'agent

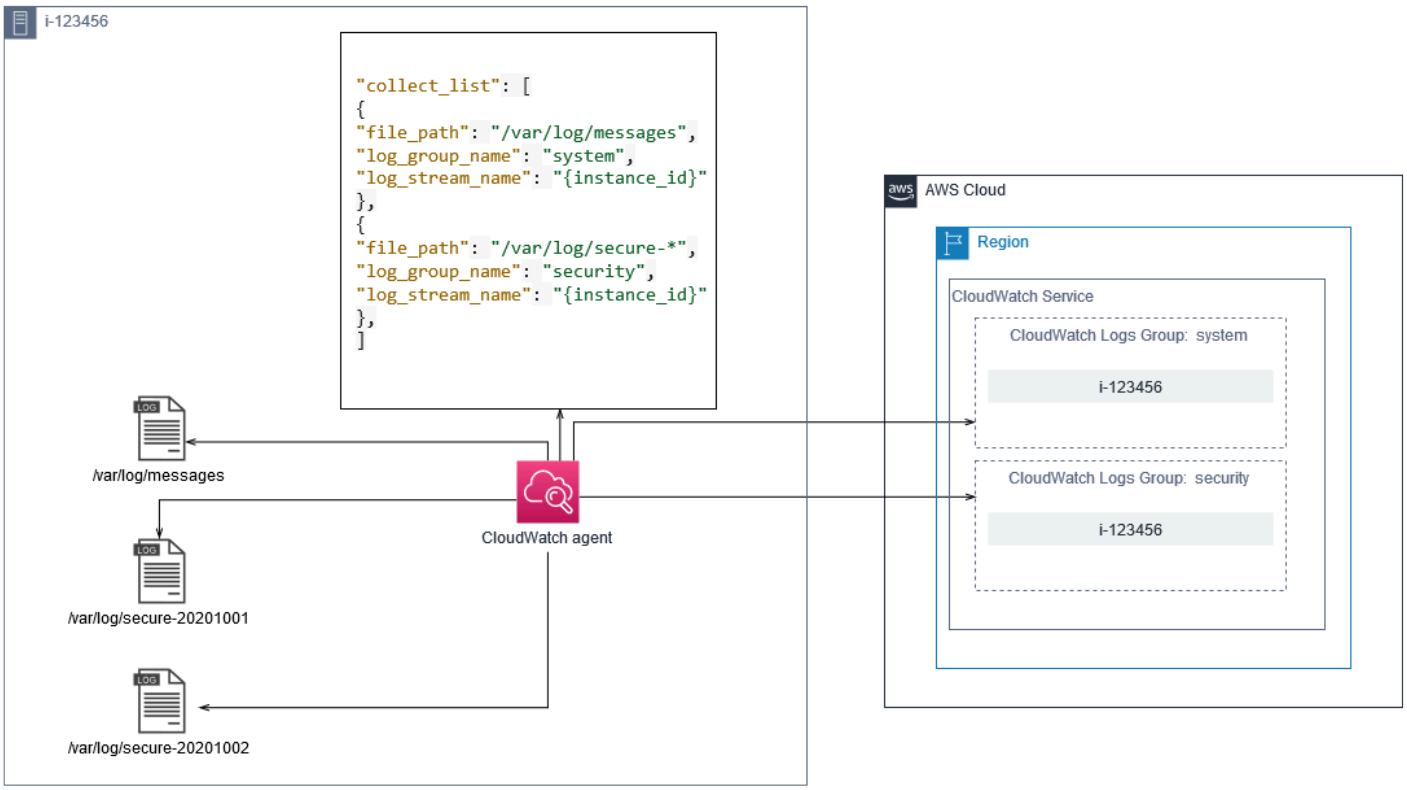
installé sur votre instance EC2,AWSAPI, ouAWS Command Line Interface(AWS CLI). Nous vous recommandons d'utiliser le CloudWatch agent pour ingérer des fichiers journaux dans CloudWatch Journaux pour Amazon EC2 et les serveurs sur site.

Vous pouvez rechercher et filtrer les journaux, ainsi que extraire des mesures et exécuter une automatisation basée sur la correction de motifs à partir de fichiers journaux dans CloudWatch. CloudWatch prend en charge les options de filtre et de syntaxe de motif en texte brut, délimité par des espaces et au format JSON, avec des 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 de texte brut.

Le CloudWatch l'agent utilise un fichier de configuration qui définit les journaux et les mesures à envoyer à CloudWatch. CloudWatch puis capture chaque fichier journal sous la forme d'unflux de journauxet regroupe ces flux de journaux dans ungroupe de journaux. Cela vous aide à effectuer des opérations sur les journaux à partir de vos instances EC2, telles que la recherche d'une chaîne correspondante.

Le nom du flux de journaux par défaut est identique à l'ID d'instance EC2 et le nom du groupe de journaux par défaut est identique au chemin d'accès au fichier journal. Le nom du flux de journaux doit être unique dans la CloudWatch groupe de journaux. Vous pouvez utiliser`instance_id`,`hostname`,`local_hostname`, ou`ip_address`pour la substitution dynamique dans le flux de journaux et les noms de groupes de journaux, ce qui signifie que vous pouvez l'utiliser CloudWatch fichier de configuration d'agent sur plusieurs instances EC2.

Le diagramme suivant illustre un CloudWatch configuration de l'agent pour capturer les journaux. Le groupe de journaux est défini par les fichiers journaux capturés et contient des flux de journaux distincts pour chaque instance EC2, car le`{instance_id}`est utilisée pour le nom du flux de journaux et les ID d'instance EC2 sont uniques.



Les groupes de journaux définissent la rétention, les balises, la sécurité, les filtres de mesures et l'étendue de recherche des flux de journaux qu'ils contiennent. Le comportement de regroupement par défaut basé sur le nom du fichier journal permet de rechercher, de créer des mesures et d'alerter les données spécifiques à un fichier journal sur les instances EC2 d'un compte et d'une région. Vous devez évaluer si un affinement supplémentaire du groupe de journaux est nécessaire. Par exemple, votre compte peut être partagé par plusieurs unités commerciales et avoir des propriétaires techniques ou d'opérations différents. 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 dépannage sur l'instance EC2 pertinente.

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 de groupe 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 journaux	`<EC2 instance ID>`

Vous pouvez également regrouper tous les fichiers journaux d'une instance EC2 dans le même groupe de journaux. Cela facilite la recherche et l'analyse dans un ensemble de fichiers journaux pour une seule instance EC2. Cela est utile si la plupart de vos instances EC2 desservent une application ou une charge de travail et que chaque instance EC2 répond à un objectif spécifique. Le tableau suivant montre comment votre nom de groupe de journaux et de flux de journaux peuvent être formatés 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 journaux	`<Log file name>`

Configuration de la capture de mesures pour les instances EC2

Par défaut, vos instances EC2 sont activées pour la surveillance basique etensemble de mesures standard(par exemple, métriques liées au processeur, au réseau ou au stockage) est automatiquement envoyée à CloudWatch toutes les cinq minutes. CloudWatch Les métriques peuvent varier selon la famille d'instances, par exemple,instances à capacité variabledisposer de mesures pour les crédits CPU. Les mesures standard Amazon EC2 sont incluses dans le prix de votre instance. Si vous activezsurveillance minutieusepour vos instances EC2, vous pouvez recevoir des données sur des périodes d'une minute. La fréquence de la période a un impact sur vos coûts CloudWatch. Assurez-vous donc d'évaluer si une surveillance détaillée est requise pour toutes les instances EC2 ou uniquement pour certaines de vos instances EC2. Par exemple, vous pouvez activer la surveillance détaillée des charges de travail de production, mais utiliser une surveillance de base pour les charges de travail autres que la production.

Les serveurs locaux n'incluent aucune mesure par défaut pour CloudWatch et doit utiliser le CloudWatch agent,AWS CLI, ouAWSSDK pour capturer des mesures. Cela signifie que vous devez définir les mesures que vous souhaitez capturer (par exemple, l'utilisation de l'UC) dans le CloudWatch fichier de configuration. Vous pouvez créer un CloudWatch fichier de configuration qui

inclut les mesures d'instance EC2 standard pour vos serveurs locaux et qui l'appliquent en plus de votre norme CloudWatch Configuration .

Métriquesdans CloudWatch sont uniquement définis par un nom de métrique et aucune ou plusieurs dimensions, et sont uniquement regroupés dans un espace de noms de métriques. Mesures fournies par unAWSle service possède un espace de noms qui commence par`AWS`(par exemple,`AWS/EC2`), et non -AWSLes métriques sont considérées comme des métriques personnalisées. Mesures que vous configurez et capturez avec le CloudWatch sont tous considérés comme des mesures personnalisées. Parce que le nombre de mesures créées a un impact sur votre CloudWatch , vous devez évaluer si chaque mesure est requise pour toutes les instances EC2 ou seulement pour certaines de vos instances EC2. Par exemple, vous pouvez définir un ensemble complet de mesures pour les charges de travail de production, mais utiliser un sous-ensemble plus petit de ces mesures pour les charges de travail hors production.

`CWAgent`est l'espace de noms par défaut des mesures publiées par le CloudWatch agent. Comme pour les groupes de journaux, l'espace de noms de mesures organise un ensemble de mesures afin qu'elles puissent être trouvées ensemble au même endroit. Vous devez modifier l'espace de noms pour refléter une unité commerciale, un projet ou une application et un environnement (par exemple,`/<Business unit>/<Project or application name>/<Environment>`). Cette approche est utile si plusieurs charges de travail non liées utilisent le même compte. Vous pouvez également corréler votre convention de dénomination d'espace de noms avec votre CloudWatch convention de dénomination des groupes de journaux.

Les mesures sont également identifiées par leurs dimensions, ce qui vous aide à les analyser par rapport à un ensemble de conditions et sont les propriétés sur lesquelles les observations sont enregistrées. Amazon EC2 inclutMétriques distinctespour les instances EC2 avec`InstanceId`et`AutoScalingGroupName`dimensions. Vous recevez également des mesures avec le`ImageId`et`InstanceType`si vous activez la surveillance détaillée. Par exemple, Amazon EC2 fournit une mesure d'instance EC2 distincte pour l'utilisation du processeur avec le`InstanceId`, en plus de la mesure d'utilisation du processeur distincte pour le`InstanceType`Dimension. Cela vous aide à analyser l'utilisation du processeur pour chaque instance EC2 unique, en plus de toutes les instances EC2 d'une instance spécifique.type d'instance.

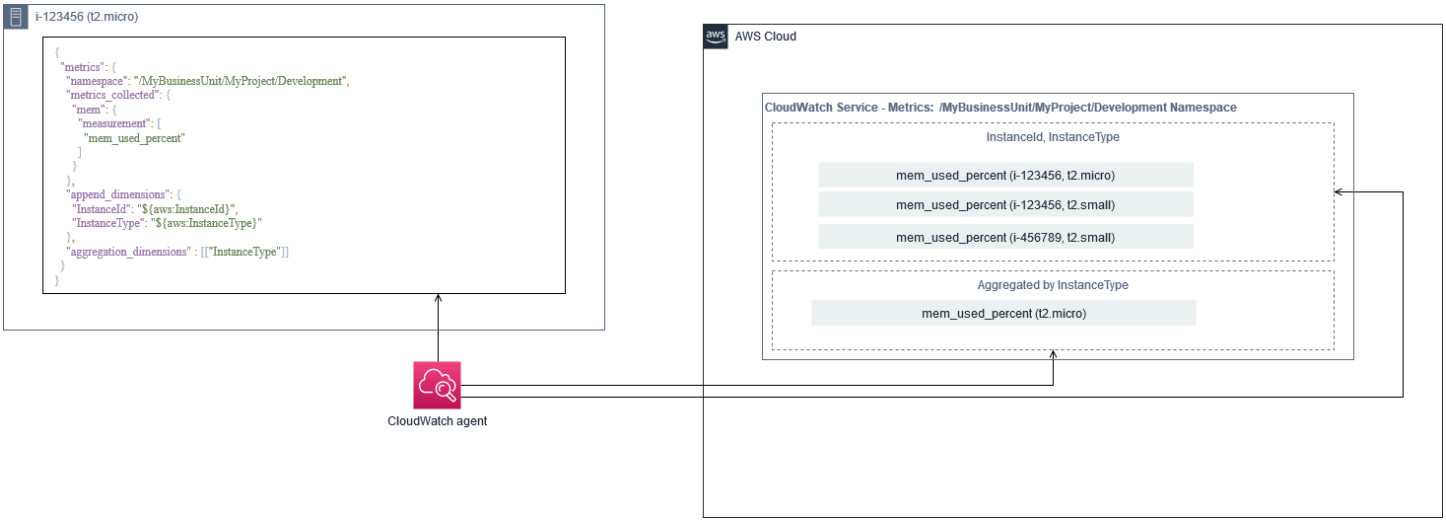
L'ajout de dimensions augmente votre capacité d'analyse, mais augmente également vos coûts globaux, car chaque mesure et chaque combinaison de valeurs de dimension unique aboutissent à une nouvelle mesure. Par exemple, si vous créez une mesure pour le pourcentage d'utilisation de la mémoire par rapport au`InstanceId`, il s'agit alors d'une nouvelle mesure pour chaque instance EC2. Si votre organisation exécute des milliers d'instances EC2, cela entraîne des milliers de

mesures et entraîne des coûts plus élevés. Pour contrôler et prédire 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 vos mesures de charge de travail de production, mais un sous-ensemble plus petit de ces dimensions pour les charges de travail autres que la production.

Vous pouvez utiliser le pluginappend_dimensionspour ajouter des dimensions à une ou à toutes les mesures définies dans votre CloudWatch Configuration . Vous pouvez également ajouter dynamiquement le`ImageId`,`InstanceId`,`InstanceType`, et`AutoScalingGroupName`à toutes les mesures de votre CloudWatch Configuration . Vous pouvez également ajouter un nom et une valeur de dimension arbitraires pour des mesures spécifiques à l'aide de la commandeappend_dimensionssur cette mesure. CloudWatch peut également agréger des statistiques sur les dimensions métriques que vous avez définies avec leaggregation_dimensionspropriété.

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

Le schéma suivant illustre un exemple CloudWatch configuration de mesures utilisant un espace de noms personnalisé, des dimensions ajoutées et une agrégation par`InstanceType`.



Niveau système CloudWatch configuration

Les métriques et les journaux au niveau des systèmes sont un composant central d'une solution de surveillance et de journalisation, et le CloudWatch l'agent dispose d'options de configuration spécifiques pour Windows et Linux.

Nous vous recommandons d'utiliser leAssistant de fichier de configuration CloudWatchou un schéma de fichier de configuration pour définir le CloudWatch fichier de configuration de l'agent pour chaque système d'exploitation que vous envisagez de prendre en charge. Des journaux et mesures supplémentaires spécifiques à la charge de travail au niveau du système d'exploitation peuvent être définis dans des paramètres distincts CloudWatch fichiers de configuration 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 instances EC2. Un exemple de configuration de compartiment S3 à cette fin est décrit dans leGestion des CloudWatch configurationssection de ce guide. Vous pouvez récupérer et appliquer automatiquement ces configurations à l'aide de State Manager et Distributor.

Configurer les journaux de niveau système

Les journaux au niveau système sont essentiels pour diagnostiquer et résoudre les problèmes sur site ou sur le siteAWSCloud. Votre approche de capture de 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.

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

Les journaux du système, des applications et de la 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 la`/etc/rsyslog.conf`ou`/etc/syslog.conf`pour déterminer la configuration spécifique des fichiers journaux de votre système.

Distribution 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 système général
	`/var/log/cron*` — Journaux Cron
	`/var/log/cloud-init-output.log` — Données de`Userdata`scripts de démarrage
Debian (Ubuntu)	`/var/log/syslog` — Journal de démarrage
	`/var/log/cloud-init-output.log` — Données de`Userdata`scripts de démarrage
	`/var/log/auth.log` — Journal de sécurité et d'authentification
	`/var/log/kern.log` — Journal du noyau

Votre organisation peut également avoir d'autres agents ou composants 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 de fichier. Par exemple, vous devez inclure le Systems Manager et CloudWatch l'agent se connecte à votre configuration. Le tableau suivant fournit l'emplacement de ces journaux d'agents pour Windows et Linux.

Windows	Agent CloudWatch	`$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	Agent CloudWatch	/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 le fichier journal est défini dans le CloudWatch configuration de l'agent, mais introuvable. Cela est utile lorsque vous souhaitez conserver une configuration de journal unique pour Linux, au lieu de configurations distinctes pour chaque distribution. Il est également utile lorsqu'un fichier journal n'existe pas tant que l'agent ou l'application logicielle commence à s'exécuter.

Configuration des métriques au niveau du système

L'utilisation de la mémoire et de l'espace disque ne sont pas incluses dans les mesures standard fournies par Amazon EC2. Pour inclure ces métriques, vous devez installer et configurer l' CloudWatch agent sur vos instances EC2. Le CloudWatch l'assistant de configuration de l'agent crée un CloudWatch configuration avecMétriques prédéfinieset vous pouvez ajouter ou supprimer des

métriques si nécessaire. Assurez-vous d'examiner les jeux de mesures prédéfinis pour déterminer le niveau approprié dont vous avez besoin.

Les utilisateurs finaux et les propriétaires de charges de travail doivent publier des mesures système supplémentaires basées sur des exigences spécifiques pour un serveur ou une instance EC2. Ces définitions de mesures doivent être stockées, versionnées et conservées dans un autre CloudWatch fichier de configuration de l'agent, partagé dans un emplacement central (par exemple, Amazon S3) à des fins de réutilisation et d'automatisation.

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

Niveau application CloudWatch configuration

Les journaux et les mesures des applications sont générés par l'exécution d'applications et sont spécifiques aux applications. Assurez-vous de définir les journaux et les mesures nécessaires pour surveiller adéquatement les applications régulièrement utilisées par votre organisation. Par exemple, votre organisation peut avoir normalisé Microsoft Internet Information Server (IIS) pour les applications Web. Vous pouvez créer un journal et une mesure standard CloudWatch configuration pour IIS qui peut également être utilisée dans l'ensemble de votre organisation. Les fichiers de configuration spécifiques à une application peuvent être stockés dans un emplacement centralisé (par exemple, un compartiment S3) et sont accessibles par les propriétaires de charges de travail ou via une récupération automatisée, puis copiés dans le CloudWatch répertoire de configuration. Le CloudWatch agent combine automatiquement les fichiers de configuration CloudWatch présents dans le répertoire des fichiers de configuration de chaque instance ou serveur EC2 en un composite CloudWatch Configuration . Le résultat final est un CloudWatch configuration qui inclut la configuration standard au niveau système de votre organisation, ainsi que tous les niveaux applicatifs pertinents CloudWatch configurations.

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

Configuration des journaux au niveau de l'application

La journalisation au niveau de l'application varie selon que l'application est commerciale. off-the-shelf (COTS) ou 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. Toutefois, la plupart des applications COTS ou tierces ne vous permettent pas de modifier fondamentalement la journalisation (par exemple, mettre à jour le code de l'application pour inclure des instructions de journal supplémentaires ou des formats non configurables). Au minimum, vous devez configurer les options de journalisation pour les applications COTS ou tierces afin de consigner les informations d'avertissement et d'erreur, de préférence au format JSON.

Vous pouvez intégrer des applications développées sur mesure avec CloudWatch Journaux en incluant les fichiers journaux de l'application dans votre CloudWatch Configuration . Les applications personnalisées offrent une meilleure qualité et un meilleur contrôle des journaux, car vous pouvez personnaliser le format de sortie du journal, classer et séparer la sortie des composants en fichiers journaux séparés, en plus d'inclure tous les détails supplémentaires requis. Assurez-vous d'examiner et de standardiser les bibliothèques de journalisation ainsi que les données et la mise en forme requises pour votre organisation afin que l'analyse et le traitement deviennent plus faciles.

Vous pouvez également écrire à un CloudWatch Flux de journaux avec CloudWatch Journaux`PutLogEvents`Appel d'API ou en utilisant leAWSKIT SDK. Vous pouvez utiliser l'API ou le SDK pour les exigences de journalisation personnalisées, telles que la coordination de la journalisation vers un flux de journaux unique sur un ensemble distribué de composants et de serveurs. Cependant, la solution la plus facile à entretenir et la plus largement applicable consiste à configurer vos applications pour qu'elles écrivent dans des fichiers journaux, puis utilisent le CloudWatch agent pour lire et diffuser les fichiers journaux sur CloudWatch.

Vous devez également prendre en compte le type de mesures que vous souhaitez mesurer à partir des fichiers journaux de vos applications. Vous pouvez utiliser des filtres de mesure pour mesurer, dessiner et alarmer ces données dans un CloudWatch groupe de journaux. Par exemple, vous pouvez utiliser un filtre de mesure pour compter les tentatives de connexion échouées en les identifiant dans vos journaux.

Vous pouvez également créer des mesures personnalisées pour vos applications développées sur mesure à l'aide duMétrique intégrée CloudWatchformatdans les fichiers journaux de votre application.

Configuration des métriques au niveau des applications

Les mesures personnalisées sont des mesures qui ne sont pas directement fournies parAWSservices pour CloudWatch et ils sont publiés dans un espace de noms personnalisé dans CloudWatch métriques , Toutes les mesures d'application sont considérées comme personnalisées CloudWatch métriques , Les mesures d'application peuvent s'aligner sur une instance EC2, 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 mesures. Les dimensions avec une grande cardinalité génèrent un grand nombre de mesures personnalisées et pourraient augmenter votre CloudWatch coûts AWS.

CloudWatch vous aide à capturer des mesures au niveau de l'application de plusieurs manières, notamment les suivantes :

- Capturez les mesures au niveau du processus en définissant les processus individuels que vous souhaitez capturer à partir de laplug-in procstat.
- Une application publie une mesure sur Windows Performance Monitor et cette mesure est définie dans le CloudWatch Configuration .
- Les filtres et modèles de mesures sont appliqués aux journaux d'une application dans CloudWatch.
- Une application écrit sur un CloudWatch en utilisant le CloudWatch format de métrique intégrée.
- Une application envoie une mesure à CloudWatch via l'API ouAWSKIT SDK.
- Une application envoie une mesure à uncollectéouStatsDdémon avec une configuration CloudWatch agent.

Vous pouvez utiliser procstat pour surveiller et mesurer les processus applicatifs critiques avec l'agent CloudWatch. Cela vous aide à déclencher une alarme et à agir (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 de vos processus applicatifs et déclencher une alarme si un processus particulier agit de façon anormale.

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

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

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

Pour les applications développées sur mesure, collaborez avec les développeurs de l'application afin de définir des mesures importantes pouvant être implémentées à l'aide du CloudWatch format de métrique intégrée,AWSKits SDK ouAWSAPI. L'approche recommandée consiste à utiliser le format de métrique intégrée. Vous pouvez utiliser le pluginAWSa fourni des bibliothèques de formats de mesures intégrées open source pour vous aider à écrire vos instructions dans le format requis. Vous devez également mettre à jour votrespécifique à l'application CloudWatch configurationpour inclure l'agent de format de métrique intégré. Cela oblige l'agent exécuté sur l'instance EC2 à agir en tant que point de terminaison au format de mesure intégré local qui envoie des mesures de format de mesure intégrées à CloudWatch.

Si vos applications prennent déjà en charge la publication de mesures à collecter ou à démarrer, vous pouvez les exploiter pour ingérer des mesures dans CloudWatch.

Approches d'installation de l'agent CloudWatch pour Amazon EC2 et les serveurs locaux

Automatisation de l' CloudWatch Le processus d'installation de l'agent vous aide à le déployer rapidement et de manière cohérente et à capturer les journaux et les mesures nécessaires. Il existe plusieurs approches pour automatiser l'installation de l'agent CloudWatch, y compris la prise en charge multi-comptes et multi-régions. Les approches d'installation automatisées suivantes sont discutées :

- Installation de CloudWatch agent utilisant Systems Manager Distributor et Systems Manager State Manager— Nous vous recommandons d'utiliser cette approche si vos instances EC2 et vos serveurs locaux exécutent l'agent Systems Manager. Cela garantit que le CloudWatch est maintenu à jour et vous pouvez générer des rapports sur des serveurs qui ne disposent pas de l'option CloudWatch agent. Cette approche évolue également pour prendre en charge plusieurs comptes et régions.
- Déploiement de l' CloudWatch agent dans le cadre du script de données utilisateur pendant le provisionnement d'instance EC2— Amazon EC2 vous permet de définir un script de démarrage exécuté lorsque vous démarrez ou redémarrez pour la première fois. Vous pouvez définir un script pour automatiser le processus de téléchargement et d'installation de l'agent. Cela peut également être inclus dansAWS CloudFormationscripts etAWSProduits 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.
- Inclusion de l'agent CloudWatch dans Amazon Machine Images (AMI)— Vous pouvez installer l'agent CloudWatch dans vos AMI personnalisées pour Amazon EC2. L'agent est automatiquement installé et démarré dans les instances EC2 qui utilisent l'AMI. Toutefois, vous devez vous assurer que l'agent et sa configuration sont régulièrement mises à jour.

Installation de CloudWatch Agent utilisant Systems Manager Distributor et State Manager

Vous pouvez utiliser Systems Manager State Manager avec Systems Manager Distributor pour installer et mettre à jour automatiquement le CloudWatch agent sur des serveurs et des instances EC2. Le distributeur inclut le`AmazonCloudWatchAgent` AWSpackage géré qui installe la version la plus récente de l'agent CloudWatch.

Voici les prérequis pour cette approche d'installation :

- L'agent Systems Manager doit être installé et en cours d'exécution sur vos serveurs ou instances EC2. L'agent Systems Manager est préinstallé sur Amazon Linux, Amazon Linux 2 et certaines AMI. L'agent doit également être installé et configuré sur d'autres images ou sur des machines virtuelles et des serveurs locaux.
- Un rôle IAM ou des informations d'identification possédant lerequis CloudWatch et des autorisations Systems Managerdoivent être attachés à l'instance EC2 ou définis dans le fichier d'informations d'identification d'un serveur local. Par exemple, vous pouvez créer un rôle IAM qui inclut leAWSpolitiques gérées :`AmazonSSMManagedInstanceCore`pour Systems Manager et`CloudWatchAgentServerPolicy`pour CloudWatch. Vous pouvez utiliser le pluginssm-cloudwatch-instance-role.yaml AWS CloudFormationpour déployer un rôle IAM et un profil d'instance qui inclut ces deux stratégies. Ce modèle peut également être modifié pour inclure d'autres autorisations IAM standard pour vos instances EC2. Pour les serveurs ou les machines virtuelles sur site, vous devez configurer le CloudWatch Agent pour utiliserService Systems Managerconfiguré pour le serveur sur site. Pour de plus amples informations à ce sujet, veuillez consulter.Comment puis-je configurer des serveurs locaux qui utilisent l'agent Systems Manager et l'agent unifié CloudWatch pour utiliser uniquement des informations d'identification temporaires ?dans leAWSCentre de connaissances.

La liste suivante présente plusieurs avantages pour l'utilisation de l'approche Systems Manager Distributor et State Manager pour installer et maintenir le CloudWatch Agent :

- Installation automatisée pour plusieurs systèmes d'exploitation— Vous n'avez pas besoin d'écrire et de gérer un script pour chaque système d'exploitation pour télécharger et installer l'agent CloudWatch.
- Vérification automatique des mises à jour— State Manager vérifie automatiquement et régulièrement que chaque instance EC2 possède la version CloudWatch la plus récente.
- Rapports de conformité— Le tableau de bord de conformité Systems Manager indique quelles instances EC2 n'ont pas réussi à installer le package Distributor.
- Installation automatisée pour les instances EC2 récemment lancées— Les nouvelles instances EC2 lancées dans votre compte reçoivent automatiquement le CloudWatch agent.

Toutefois, vous devez également prendre en compte les trois domaines suivants avant de choisir cette approche :

- Collision avec une association existante— Si une autre association installe ou configure déjà le CloudWatch , alors les deux associations peuvent interférer l'une avec l'autre et potentiellement causer des problèmes. Lorsque vous utilisez cette approche, vous devez supprimer toutes les associations existantes qui installent ou mettent à jour l'agent et la configuration CloudWatch.
- Mise à jour des fichiers de configuration d'agent— Le distributeur effectue une installation à l'aide du fichier de configuration par défaut. Si vous utilisez un fichier de configuration personnalisé ou plusieurs fichiers CloudWatch , vous devez mettre à jour la configuration après l'installation.
- Configuration multi-régions ou multi-comptes— L'association State Manager doit être configurée dans chaque compte et chaque 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 le CloudWatch configuration afin que plusieurs comptes et régions puissent récupérer et appliquer les normes requises.

Configurer State Manager et Distributor pour CloudWatch déploiement et configuration de l'agent

Vous pouvez utiliserConfiguration rapide de Systems Managerpour configurer rapidement les fonctionnalités de Systems Manager, y compris l'installation et la mise à jour automatiques du CloudWatch agent sur vos instances EC2. Le Quick Setup déploie unAWS CloudFormationstack qui déploie et configure les ressources Systems Manager en fonction de vos choix.

La liste suivante répertorie deux actions importantes effectuées par Quick Setup pour l'automatisation. CloudWatch installation et mise à jour de l'agent :

1. Création de documents personnalisés Systems Manager— La configuration rapide 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`AmazonSSMRoleForInstancesQuickSetup`le rôle et le profil d'instance s'ils n'existent pas et attachent le`AmazonSSMManagedInstanceCore`stratégie pour le rôle. Cela n'inclut pas les`CloudWatchAgentServerPolicy`Politique IAM. Vous devez mettre à jour cette stratégie et mettre à jour ce document Systems Manager pour inclure cette stratégie, comme décrit dans la section suivante.

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

2. Création d'associations State Manager— Les associations State Manager sont créées et configurées pour utiliser les documents Systems Manager personnalisés créés. Les noms d'association State Manager peuvent varier, mais la configuration reste la même :
   - `ManageCloudWatchAgent`— Exécutions de l'`InstallAndManageCloudWatchDocument`Document Systems Manager une fois pour chaque instance EC2.
   - `UpdateCloudWatchAgent`— Exécutions de l'`UpdateCloudWatchDocument`Document Systems Manager tous les 30 jours pour chaque instance EC2.
   - Exécutions de l'`CreateAndAttachIAMToInstance`Document Systems Manager une fois pour chaque instance EC2.

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

> **Important**
>
> La configuration rapide crée unAWS CloudFormationpour déployer et configurer les ressources Systems Manager en fonction de vos choix. Si vous mettez à jour vos choix de configuration rapide, vous devrez peut-être réactualiser manuellement les documents Systems Manager.

Les sections suivantes décrivent comment mettre à jour manuellement les ressources Systems Manager créées par Quick Setup, et utiliser les vôtresAWS CloudFormationmodèle pour effectuer une configuration rapide mise à jour. Nous vous recommandons d'utiliser votre propreAWS CloudFormationpour éviter de mettre à jour manuellement les ressources créées par Quick Setup etAWS CloudFormation.

Utiliser la configuration rapide de Systems Manager et mettre à jour manuellement les ressources Systems Manager créées

Les ressources de Systems Manager créées par l'approche Quick Setup doivent être mises à jour pour inclure les ressources requises CloudWatch autorisations d'agent et prise en charge de plusieurs CloudWatch fichiers de configuration. Cette section explique comment mettre à jour le rôle IAM et les documents Systems Manager pour utiliser un compartiment S3 centralisé contenant CloudWatch configurations accessibles depuis plusieurs comptes. Création d'un compartiment S3 pour stocker le CloudWatch Les fichiers de configuration sont décrits dans leGestion des CloudWatch configurationsde ce guide.

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

Ce document Systems Manager créé par Quick Setup vérifie si un profil d'instance IAM existant est attaché à une instance EC2. Si c'est le cas, il attache le`AmazonSSMManagedInstanceCore`la stratégie du rôle de existant. Cela protège vos instances EC2 existantes contre les pertesAWSautorisations pouvant être attribuées via des profils d'instance existants. Vous devez ajouter une étape dans ce document pour joindre le`CloudWatchAgentServerPolicy`Stratégie IAM pour les instances EC2 auxquelles un profil d'instance est déjà attaché. Le document Systems Manager crée également le rôle IAM s'il n'existe pas et qu'aucune instance EC2 n'est associée à un profil d'instance. Vous devez mettre à jour cette section du document pour inclure également le`CloudWatchAgentServerPolicy`Politique IAM.

Vérifiez le produit terminéCréer et attacher une instance à l'instance .yamlexemple de document 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 Quick Setup peut être différent de l'exemple de document fourni. Assurez-vous donc d'effectuer les ajustements nécessaires. L'exemple de document inclut le choix d'option Quick Setup pour analyser quotidiennement les instances à la recherche de correctifs manquants. Il inclut donc une stratégie pour Systems Manager Patch Manager.

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

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

Vérifiez le produit terminéInstaller et gérer Cloud Watch Document.yamldocument mis à jour et comparez-le au document créé par Quick Setup. Le document créé par votre configuration rapide peut être différent. Assurez-vous donc d'avoir effectué les ajustements nécessaires. Modifiez votre document existant pour inclure les étapes et les modifications nécessaires.

UtiliserAWS CloudFormationau lieu de la configuration rapide

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

La fonction Quick Setup utilise égalementAWS CloudFormationet crée unAWS CloudFormationensemble de pile pour déployer et configurer les ressources Systems Manager en fonction de vos choix. Avant de pouvoir utiliserAWS CloudFormation, vous devez créer les rôles IAM utilisés parAWS CloudFormation StackSets pour prendre en charge les déploiements sur plusieurs comptes ou régions. La configuration rapide crée les rôles dont elle a besoin pour prendre en charge les déploiements multi-régions ou multi-comptes avecAWS CloudFormationStackSets. Vous devez remplir les prérequis pourAWS CloudFormation StackSets si vous souhaitez configurer et déployer des ressources Systems Manager dans plusieurs régions ou plusieurs comptes à partir d'un seul compte et d'une même région. Pour de plus amples informations à ce sujet, veuillez consulter.Prérequis pour les opérations sur les ensembles de pilesdans leAWS CloudFormation.

Vérifiez leAWS - QuickSetup - SSMHOSTMGMT.YAML AWS CloudFormationModèle pour la configuration rapide personnalisée.

Vous devez passer en revue les ressources et les capacités duAWS CloudFormationCréez des modèles et apportez des ajustements en fonction de vos besoins. Vous devez contrôler la

versionAWS CloudFormationmodèle que vous utilisez et testez incrémentiellement les modifications pour confirmer le résultat requis. En outre, vous devez effectuer des examens de sécurité dans le cloud pour déterminer si des ajustements de stratégie sont nécessaires en fonction des exigences de votre organisation.

Vous devez déployer leAWS CloudFormationempilez dans un seul compte de test et une région, et effectuez tous les cas de test nécessaires pour personnaliser et confirmer le résultat souhaité. Vous pouvez ensuite graduer votre déploiement vers plusieurs régions dans un même compte, puis vers plusieurs comptes et plusieurs régions.

Configuration rapide personnalisée dans un seul compte et une seule région avec unAWS CloudFormationempiler

Si vous n'utilisez qu'un seul compte et une seule région, vous pouvez déployer l'exemple complet en tant queAWS CloudFormationpile au lieu d'unAWS CloudFormationensemble de piles Toutefois, si possible, nous vous recommandons d'utiliser l'approche de jeu de piles multi-comptes et multi-régions, même si vous n'utilisez qu'un seul compte et une seule région. A l'aide deAWS CloudFormation StackSets facilite l'extension à d'autres comptes et régions à l'future.

Procédez comme suit pour déployer leAWS - QuickSetup - SSMHOSTMGMT.YAML AWS CloudFormationmodèle comme unAWS CloudFormationcumuler dans un seul compte et une seule région :

1. Téléchargez le modèle et enregistrez-le dans votre système de contrôle de version préféré (par exemple,AWS CodeCommit).
2. Personnalisation de la valeur parAWS CloudFormationvaleurs de paramètres basées sur les exigences de votre organisation.
3. Personnalisez les programmes d'association State Manager.
4. Personnalisez le document Systems Manager avec le`InstallAndManageCloudWatchDocument`ID logique. Vérifiez que les préfixes du compartiment S3 sont alignés sur les préfixes du compartiment S3 contenant votre CloudWatch Configuration .
5. Récupérez et enregistrez l'Amazon Resource Name (ARN) du compartiment S3 contenant votre CloudWatch configurations. Pour de plus amples informations à ce sujet, veuillez consulter leGestion des CloudWatch configurationsde ce guide. Un échantilloncloudwatch-config-s3-bucket.yaml AWS CloudFormationest disponible qui inclut une stratégie de compartiment pour fournir un accès en lecture àAWS Organizationscomptes.

6. Déployez la configuration rapide personnaliséeAWS CloudFormationModèle sur le même compte que votre compartiment S3 :
   - Pour`CloudWatchConfigBucketARN`, saisissez l'ARN du compartiment S3.
   - Apportez des ajustements aux options de paramètres en fonction des fonctionnalités que vous souhaitez activer pour Systems Manager.

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

- Appliquez le`AttachIAMToInstance`Associations State Manager. Il s'agit d'un runbook Systems Manager configuré pour être exécuté selon la planification. Les associations State Manager qui utilisent des runbooks ne sont pas automatiquement appliquées aux nouvelles instances EC2 et peuvent être configurées pour être exécutées sur une base planifiée. Pour de plus amples informations, veuillez consulterExécution d'automatisations avec des déclencheurs en utilisant State Managerdans la documentation Systems Manager.
- Vérifiez que le rôle IAM requis est attaché à l'instance EC2.
- Vérifiez que l'agent Systems Manager fonctionne correctement en confirmant que l'instance EC2 est visible dans Systems Manager.
- Confirmer que le CloudWatch l'agent fonctionne correctement en affichant CloudWatch journaux et métriques basés sur le CloudWatch configurations à partir de votre compartiment S3.

Configuration rapide personnalisée dans plusieurs régions et comptes avecAWS CloudFormationStackSets

Si vous utilisez plusieurs comptes et régions, vous pouvez déployer leAWS - QuickSetup - SSMHOSTMGMT.YAML AWS CloudFormationmodèle en tant qu'ensemble de pile. Vous devez remplir leAWS CloudFormationPrérequis de StackSetavant d'utiliser des jeux de pile. Les exigences varient selon que vous déployez des jeux de piles avecautogéréougestion par serviceautorisations.

Nous vous recommandons de déployer des jeux de piles avec des autorisations gérées par le service afin que les nouveaux comptes reçoivent automatiquement la configuration rapide personnalisée. Vous devez déployer un ensemble de piles gérées par le service à partir duAWS Organizationscompte de gestion ou compte d'administrateur délégué. Vous devez déployer le jeu de piles à partir d'un compte centralisé utilisé pour l'automatisation qui dispose de privilèges d'administrateur délégués, plutôt que leAWS Organizationscompte de gestion Nous vous

recommandons également de tester le déploiement de votre jeu de piles en ciblant une unité organisationnelle de test (UO) avec un nombre unique ou restreint de comptes dans une même région.

1. Terminez les étapes 1 à 5 duConfiguration rapide personnalisée dans un seul compte et une seule région avec unAWS CloudFormationempilerde ce guide.
2. Connectez-vous à la consoleAWS Management Console, ouvrezAWS CloudFormationconsoler et choisirCréer un StackSet :
   - ChoisissezTemplate is ready (Le modèle est prêt)etCharger un fichier de modèle. Chargez leAWS CloudFormationmodèle que vous avez personnalisé en fonction de vos besoins.
   - Spécifiez les détails du jeu de piles :
     - Entrez un nom de pile, par exemple,`StackSet-SSM-QuickSetup`.
     - Apportez des ajustements aux options de paramètres en fonction des fonctionnalités que vous souhaitez activer pour Systems Manager.
     - Pour`CloudWatchConfigBucketARN`, saisissez l'ARN de votre CloudWatch compartiment S3 de la configuration.
     - Spécifiez les options du jeu de piles, choisissez si vous allez utiliser les autorisations gérées par le service avecAWS Organizationsou des autorisations autogérées.
       - Si vous choisissez des autorisations autogérées, entrez le champRôle d'administration d'AWS Cloud Formations StacksetetRôle d'exécution d'AWS Cloud Formations StacksetDétails des rôles IAM. Le rôle d'administrateur doit exister dans le compte et le rôle d'exécution doit exister dans chaque compte cible
     - Pourgestion par serviceAutorisations avecAWS Organizations, nous vous recommandons de commencer par déployer vers une unité d'organisation de test au lieu de l'ensemble de l'organisation.
       - Décidez si vous voulez activer les déploiements automatiques. Nous vous recommandons de choisirActivé. Pour ce qui est du comportement de suppression de compte, le paramètre recommandé estSupprimer des piles.
     - Pourautogéréautorisations, saisissez leAWSID de compte des comptes que vous voulez 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 a réussi en affichant l'état dans leOpérations etInstances de pilespour le jeu de piles.

- Testez que Systems Manager et CloudWatch fonctionnent correctement dans les comptes déployés en suivant l'étape 7 duConfiguration rapide personnalisée dans un seul compte et une seule région avec unAWS CloudFormationempilerde ce guide.

Considérations relatives à la configuration des serveurs locaux

Le CloudWatch agent pour serveurs locaux et machines virtuelles est installé et configuré en utilisant une approche similaire à celle des instances EC2. Toutefois, le tableau suivant fournit des considérations que vous devez évaluer lors de l'installation et de la configuration de l' CloudWatch sur des serveurs et des machines virtuelles sur site.

Pointez le CloudWatch avec les mêmes informations d'identification temporaires que celles utilisées pour Systems Manager.	Lorsque vous configurez Systems Manager dans un environnement hybride comprenant des serveurs locaux, vous pouvez activer Systems Manager avec un rôle IAM. Vous devez utiliser le rôle créé pour vos instances EC2 qui inclut le`CloudWatchAgentServerPolicy` et`AmazonSSMManagedInstanceCore` politiques. L'agent Systems Manager récupère et écrit des informations d'identification temporaires dans un fichier d'informations d'identification local. Vous pouvez pointer votre CloudWatch configuration de l'agent dans le même fichier. Vous pouvez utiliser le processus à partir deConfigurer des serveurs locaux qui utilisent l'agent Systems Manager et l'agent CloudWatch unifié pour utiliser uniquement des informations d'identification temporairesdans leAWSCentre de connaissances. Vous pouvez également automatiser ce processus en définissant un runbook Systems Manager Automation et une association State Manager distincts, et en ciblant vos

	instances locales avec des balises. Lorsque vous créez unActivation Systems Managerpour vos instances locales, vous devez inclure une balise qui identifie les instances en tant qu'instances locales.
Envisagez d'utiliser des comptes et des régions dotés d'un VPN ouAWS Direct ConnectAccès etAWSPrivateLink.	Vous pouvez utiliserAWS Direct Connectou AWS Virtual Private Network(AWS VPN) pour établir des connexions privées entre les réseaux locaux et votre cloud privé virtuel (VPC).AWS PrivateLink établit une connexion privée à CloudWatch Journaux avec un point de terminaison d'un VPC d'interface. Cette approche est utile si vous avez des restrictions qui empêchent l'envoi de données sur Internet public vers un point de terminaison de service public.
Toutes les mesures doivent être incluses dans le CloudWatch fichier de configuration.	Amazon EC2 inclut des mesures standard (par exemple, utilisation du processeur), mais ces mesures doivent être définies pour les instances locales. 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 norme. CloudWatch configuration des métriques pour la plateforme.

Considérations relatives aux instances EC2 éphémères

Les instances EC2 sont temporaires, ouéphémère, s'ils sont provisionnés par Amazon EC2 Auto Scaling, Amazon EMR,Instances Spot Amazon EC2, ouAWS Batch. Les instances EC2 éphémères peuvent provoquer un très grand nombre de CloudWatch flux sous un groupe de journaux commun sans informations supplémentaires sur leur origine d'exécution.

Si vous utilisez des instances EC2 éphémères, envisagez d'ajouter des informations contextuelles dynamiques supplémentaires dans le groupe de journaux et les noms de 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 Auto Scaling. Ces informations peuvent varier pour les instances EC2 nouvellement lancées et vous devrez peut-être les récupérer et les configurer lors de l'exécution. Pour ce faire, écrivez un CloudWatch fichier de configuration de l'agent au démarrage et au redémarrage de l'agent pour inclure le fichier de configuration mis à jour. Cela permet de fournir des journaux et des mesures à CloudWatch à l'aide des informations d'exécution dynamique.

Vous devez également vous assurer que vos métriques et vos journaux sont envoyés par le CloudWatch avant que vos instances EC2 éphémères ne soient arrêtées. Le CloudWatch l'agent inclut un`flush_interval`qui peut être configuré pour définir l'intervalle de temps de vidage des tampons de journaux et de métriques. Vous pouvez réduire cette valeur en fonction de votre charge de travail et arrêter le CloudWatch et forcez les tampons à vider avant la fin de l'instance EC2.

Utilisation d'une solution automatisée pour déployer le CloudWatch agent

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

- Vérifiez que l'automatisation couvre les systèmes d'exploitation et les versions du système d'exploitation que vous prenez en charge. Si le script d'automatisation ne prend pas en charge tous les OS de votre organisation, vous devez définir des solutions alternatives pour les systèmes d'exploitation non pris en charge.
- Vérifiez que la solution d'automatisation vérifie régulièrement les mises à jour et les mises à niveau de l'agent CloudWatch. Votre solution d'automatisation doit régulièrement vérifier s'il y a des mises à jour du CloudWatch ou désinstallez et réinstallez régulièrement l'agent. Vous pouvez utiliser une fonctionnalité de planificateur ou 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 si 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 que les installations et les configurations défaillantes soient suivies.

Déploiement de l' CloudWatch agent pendant le provisionnement d'instance avec le script de données utilisateur

Vous pouvez utiliser cette approche si vous ne prévoyez pas d'utiliser Systems Manager et que vous souhaitez utiliser CloudWatch de manière sélective pour vos instances EC2. En règle générale, cette approche est utilisée en une seule fois ou lorsqu'une configuration spécialisée est requise.AWSfournitliens directspour la CloudWatch agent qui peut être téléchargé dans vos scripts de démarrage ou de données utilisateur. Les packages d'installation de l'agent peuvent être exécutés silencieusement sans interaction de l'utilisateur, ce qui signifie que vous pouvez les utiliser dans des déploiements automatisés. Si vous utilisez cette approche, vous devez évaluer les considérations suivantes :

- Risque accru que les utilisateurs n'installent pas l'agent ou ne configurent pas de mesures standard. Les utilisateurs peuvent provisionner des instances sans inclure les étapes nécessaires pour installer le 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 à différentes versions du système d'exploitation. Vous avez besoin de scripts distincts si vous avez l'intention d'utiliser Windows et Linux. Le script Linux doit également comporter différentes étapes d'installation en fonction de la distribution.
- Vous devez régulièrement mettre à jour le CloudWatch agent avec de nouvelles versions lorsqu'il est disponible. 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 réexécute au démarrage de l'instance. Le CloudWatch l'agent est ensuite mis à jour et réinstallé à chaque redémarrage.
- Vous devez automatiser la récupération et l'application des configurations CloudWatch standard. Cela peut être automatisé si vous utilisez Systems Manager avec State Manager, mais vous pouvez également configurer un script de données utilisateur pour extraire les fichiers de configuration au démarrage et redémarrer le CloudWatch agent.

Incluant le CloudWatch agent dans vos AMI

L'avantage de l'utilisation de cette approche est que vous n'avez pas à attendre la CloudWatch agent à installer et à configurer, et vous pouvez immédiatement commencer la journalisation et la surveillance. Cela vous aide à mieux surveiller les étapes de provisionnement et de démarrage

de votre instance en cas d'échec du démarrage des instances. Cette approche est également appropriée si vous ne prévoyez pas d'utiliser l'agent Systems Manager. Si vous utilisez cette approche, vous devez évaluer les considérations suivantes :

- Un processus de mise à jour doit exister car les AMI peuvent ne pas inclure la plus récente CloudWatch Version d'agent. Le CloudWatch l'agent installé dans une AMI n'est à jour que lors de la dernière création de l'AMI. Vous devez inclure une méthode supplémentaire pour mettre à jour l'agent régulièrement et lorsque l'instance EC2 est provisionnée. Si vous utilisez Systems Manager, vous pouvez utiliser leInstallation de CloudWatch Agent utilisant Systems Manager Distributor et State Managersolution fournie dans ce guide. 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.
- Votre CloudWatch le fichier de configuration de l'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 le CloudWatch agent.
- Le CloudWatch l'agent doit être redémarré après votre CloudWatch la configuration est mise à jour.
- AWSles informations d'identification ne doivent pas être enregistrées dans l'AMI. Assurez-vous qu'aucun local n'estAWSles informations d'identification sont stockées 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 le 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 AWS Fargate sont 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 lancement EC2
- Journaux de conteneurs Amazon ECS pour les types de lancement EC2 et Fargate
- Utilisation du routage personnalisé des journaux avec FireLens pour Amazon ECS
- Métriques pour Amazon ECS

Configuration CloudWatch avec un type de lancement EC2

Avec un type de lancement EC2, vous mettez en service un cluster Amazon ECS d'instances EC2 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 lancement EC2. Cela crée une AWS 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 instances EC2 décrite dans la Installation de CloudWatch Agent utilisant 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 configuration standardisée au niveau du système pour CloudWatch 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 AWS 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'instance EC2 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 ne gérez les instances de conteneur EC2.

Les instances de conteneur Amazon ECS doivent utiliser les dernières AMI optimisées pour Amazon ECS et l'agent de conteneur. 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 les dernières AMI optimisées depuis le Parameter Store en utilisant le format de paramètres Parameter Store pour les AMI optimisées Amazon ECS. 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 AWS CloudFormation modèles.

AWS fournit les mêmes paramètres de magasin de paramètres dans chaque région prise en charge. Cela signifie que les AWS 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 des nouvelles AMI Amazon ECS 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 EC2 et Fargate

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 pipeline d'intégration et de livraison continues (CI/CD) ou un processus automatisé, vous pouvez créer une nouvelle révision de la définition des tâches pour votre application à chaque nouvelle génération d'image Docker. Par exemple, vous pouvez inclure le nom de l'image Docker, la balise d'image, GitHub la révision ou d'autres informations importantes dans la révision de votre définition de tâche et dans la configuration de journalisation dans le cadre de votre processus CI/CD.

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 à partir des 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 AWS 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 CloudWatch déploiement et configuration de l'agent 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 sur Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) s'intègre à CloudWatch Journaux pour le plan de contrôle Kubernetes. Le plan de contrôle est fourni en tant que service géré par Amazon EKS et vous pouvezactiver la journalisation sans installer d'agent CloudWatch. Le CloudWatch L'agent peut également être déployé pour capturer les journaux de nœuds et de conteneurs Amazon EKS. Fluent Bit et Fluentdsont également pris en charge pour l'envoi de vos journaux de conteneur à CloudWatch Bûches.

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

Vous pouvez également Configuration de l' CloudWatch Agent pour gratter les métriques Prometheuset créer CloudWatch mesures, en plus de consommer d'autres points de terminaison Prometheus. Surveillance de Container Insights pour Prometheuspeut également détecter et capturer automatiquement les mesures Prometheus à partir de charges de travail et de systèmes conteneurisés pris en charge.

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

Journalisation pour Amazon EKS

La journalisation Kubernetes peut être divisée en journalisation du plan de contrôle, journalisation des nœuds et journalisation des applications. LePlan de contrôle Kubernetesest 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 pouvezactiver les journaux pour différents composants du plan de contrôleet envoyez-les à CloudWatch.

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

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

Les conteneurs sont regroupés comme suit :gousses dans un cluster Kubernetes et sont programmés pour être exécutés sur vos nœuds Kubernetes. La plupart des applications conteneurisées écrivent sur une sortie standard et une erreur standard, et le moteur de conteneur redirige la sortie vers un pilote de journalisation. Dans Kubernetes, les journaux de conteneurs se trouvent dans le `/var/log/pods` répertoire sur un nœud. Vous pouvez configurer CloudWatch et 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 se compose d'un plan de contrôle à locataire unique haute disponibilité pour votre cluster Kubernetes et les nœuds Amazon EKS qui exécutent vos conteneurs. Les nœuds du plan de contrôle exécutés dans un compte géré parAWS. Les nœuds du plan de contrôle de cluster Amazon EKS sont intégrés aux CloudWatch et vous pouvez activer la journalisation pour des composants spécifiques du plan de contrôle.

Les journaux sont fournis pour chaque instance de composant du plan de contrôle Kubernetes.AWSgère l'état de santé des nœuds de votre plan de contrôle et fournit unaccord de niveau de service (SLA) pour le point de terminaison Kubernetes.

Journalisation des nœuds et des applications Amazon EKS

Nous vous recommandons d'utiliserCloudWatch Container Insightspour capturer des journaux et des mesures pour Amazon EKS. Container Insights implémente des mesures au niveau du cluster, du nœud et du pod avec le CloudWatch agent et Fluent Bit ou Fluentd pour la capture de journaux sur CloudWatch. Container Insights fournit également des tableaux de bord automatiques avec des vues en couches de vos données capturées CloudWatch métriques , Container Insights est déployé en tant que CloudWatch DaemonSet et Fluent Bit DaemonSet qui s'exécute sur tous les nœuds Amazon EKS. Les nœuds Fargate ne sont pas pris en charge par Container Insights car ils sont gérés parAWSet ne prenez pas en charge DaemonSets. La journalisation Fargate pour Amazon EKS est traitée séparément dans ce guide.

Le tableau suivant contient le CloudWatch groupes de journaux et journaux capturés par leConfiguration de capture des journaux Fluentd ou Fluent Bit par défautpour Amazon EKS.

`/aws/containerinsights/Cluster_Name/application`	Tous les fichiers journaux situés dans/`var/log/containers` . Ce répertoire fournit des liens symboliques vers tous les journaux de conteneurs Kubernetes dans le/`var/log/pods` Structure de répertoire. Cela capture les journaux de votre conteneur d'applications en écrivant dans`stdout` ou `stderr`. Il inclut également des journaux pour les conteneurs système Kubernetes tels que`aws-vpc-cni-init` ,`kube-proxy` , et`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 with Fluent Bit ou Fluentd pour la journalisation, vous pouvez capturer les journaux de nœuds et de conteneurs avec le CloudWatch Agent installé sur des nœuds Amazon EKS. Les nœuds Amazon EKS sont des instances EC2, ce qui signifie que vous devez les inclure dans votre approche de journalisation standard au niveau système pour Amazon EC2. Si vous installez le CloudWatch agent utilisant Distributor et State Manager, puis les nœuds Amazon EKS sont également inclus dans le CloudWatch installation, configuration et mise à jour de l'agent.

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

`/var/log/containers`	Ce répertoire fournit des liens symboliques vers tous les journaux de conteneurs Kubernetes sous le/`var/log/pods` Structure de répertoir

	e. Cela permet de capturer efficacement les journaux de votre conteneur d'applications en écrivant dans`stdout`ou`stderr`. Cela inclut les journaux des conteneurs système Kubernetes tels que`aws-vpc-cni-init` ,`kube-proxy` , et`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 le CloudWatch agent pour envoyer des journaux et des mesures au niveau système appropriés. Toutefois, l'AMI optimisée Amazon EKS n'inclut aucun agent Systems Manager. En utilisantmodèles de lancement, vous pouvez automatiser l'installation de l'agent Systems Manager et une installation par défaut CloudWatch configuration qui capture d'importants journaux spécifiques à Amazon EKS avec 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 quegroupe de nœuds géréou commenœuds autogérés.

Avec les groupes de nœuds gérés, vous fournissez unmodèle de lancementqui inclut la section données utilisateur pour automatiser l'installation de l'agent Systems Manager et CloudWatch Configuration . Vous pouvez personnaliser et utiliser leamazon_eks_managed_node_group_launch_config.yaml AWS CloudFormationpour créer un modèle de lancement qui installe l'agent Systems Manager, CloudWatch , et ajoute également une configuration de journalisation spécifique à Amazon EKS au CloudWatch répertoire de configuration. Ce modèle peut être utilisé pour mettre à jour votre modèle de lancement de groupes de nœuds gérés Amazon EKS avec un infrastructure-as-code (iAC). Chaque mise à jour duAWS CloudFormationfournit 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 disposer du kitprocessus de cycle de vie gérémettez à jour vos nœuds sans temps d'arrêt. Assurez-vous que le rôle et le profil d'instance IAM appliqués à votre groupe de nœuds gérés incluent le`CloudWatchAgentServerPolicy`et`AmazonSSMManagedInstanceCore` AWSpolitiques gérées.

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 etBottlerocket, avecautres options. Vous pouvez utiliserAWS CloudFormationpour déployer des nœuds autogérés dans vos clusters Amazon EKS, ce qui signifie que vous pouvez utiliser une approche iAC et des modifications gérées pour vos clusters Amazon EKS.AWSfournit leamazon-eks-nodegroup.yaml AWS CloudFormationque vous pouvez utiliser en l'état 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). Leamazon-eks-nodegroup.yaml AWS CloudFormationmodèle est une version mise à jour qui installe l'agent Systems Manager requis, CloudWatch , et ajoute également une configuration de journalisation spécifique à Amazon EKS au CloudWatch répertoire de configuration.

Enregistrement pour Amazon EKS sur Fargate

Avec Amazon EKS on Fargate, vous pouvez déployer des espaces sans allouer ni gérer vos nœuds Kubernetes. Cela élimine la nécessité de capturer des journaux au niveau système pour vos nœuds Kubernetes. Pour capturer les journaux de vos pods Fargate, vous pouvez utiliser Fluent Bit pour transférer les journaux directement vers CloudWatch. Cela vous permet d'acheminer automatiquement les journaux vers CloudWatch sans configuration supplémentaire ni conteneur sidecar pour vos pods Amazon EKS sur Fargate. Pour plus d'informations à ce sujet, veuillez consulterJournalisation Fargatedans la documentation Amazon EKS etEmbout Fluent pour Amazon EKSsur leAWSBlog. Cette solution permet de capturer le`STDOUT`et`STDERR`flux de données d'entrée/sortie (I/O) de votre conteneur et les envoie à CloudWatch via Fluent Bit, basé sur la configuration Fluent Bit établie pour le cluster Amazon EKS sur Fargate.

Métriques pour Amazon EKS et Kubernetes

Kubernetes fournit une API de mesures qui vous permet d'accéder aux mesures d'utilisation des ressources (par exemple, l'utilisation du processeur et de la mémoire pour les nœuds et les espaces), mais l'API fournit uniquement des informations ponctuelles et non des mesures historiques. LeServeur de mesures Kubernetesest généralement utilisé pour les déploiements Amazon EKS et Kubernetes pour agréger les mesures, fournir des informations historiques à court terme sur les mesures et des fonctionnalités de support telles queHorizontal Pod Autoscaler (HPA).

Amazon EKS expose les mesures du plan de contrôle via le serveur API Kubernetesau format Prometheuset CloudWatch peut capturer et ingérer ces mesures. CloudWatch et Container Insights

peuvent également être configurés pour fournir des mesures complètes de capture, d'analyse et d'alarme pour vos nœuds et espaces Amazon EKS.

Métriques du plan de contrôle Kubernetes

Kubernetes expose les mesures du plan de contrôle dans un format Prometheus à l'aide de la `/metrics` Point de terminaison de l'API HTTP. Vous devez installerPrometheusdans votre cluster Kubernetes pour tracer et visualiser ces mesures à l'aide d'un navigateur Web. Vous pouvez également ingérer les mesures exposéespar le serveur API Kubernetes dans CloudWatch.

Mesures des nœuds et des systèmes pour Kubernetes

Kubernetes fournit le PrometheusMétriques de serveurpod que vous pouvezdéploiement et exécutionsur vos clusters Kubernetes pour des statistiques sur le processeur et la mémoire au niveau du cluster, du nœud et du pod. Ces mesures sont utilisées avec leHorizontal Pod Autoscaler (HPA)etVertical Pod Autoscaler (VPA). CloudWatch peuvent également fournir ces mesures.

Vous devez installer le serveur Kubernetes Metrics Server si vous utilisez leTableau de bord Kubernetesou les autoscalers horizontaux et verticaux. Le tableau de bord Kubernetes vous aide à parcourir et à configurer votre cluster Kubernetes, vos nœuds, vos espaces et la configuration associée, et à afficher les métriques du processeur et de la mémoire à partir du serveur Kubernetes Metrics. Vous pouvez déployer cette solution pour des clusters individuels en suivant les étapes duDéploiement du tableau de bord Kubernetesdans la documentation Amazon EKS.

Les mesures fournies par Kubernetes Metrics Server ne peuvent pas être utilisées à des fins de dimensionnement non automatique (par exemple, la surveillance). Les mesures sont destinées à : point-in-time analyse et non analyse historique. Le tableau de bord Kubernetes déploie le`dashboard-metrics-scraper`pour stocker des mesures à partir du serveur Kubernetes Metrics pendant une courte période.

Container Insights utilise une version conteneurisée du CloudWatch agent qui s'exécute dans un Kubernetes DaemonSet pour découvrir tous les conteneurs en cours d'exécution dans un cluster et fournir des mesures au niveau des nœuds. Il collecte les données de performance à chaque couche de la pile de performances. Vous pouvez utiliser le Quick Start deAWSDémarrage rapide ou configurez Container Insights séparément. Quick Start configure la surveillance des métriques avec le CloudWatch 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.

Étant donné que les nœuds Amazon EKS sont des instances EC2, vous devez capturer des mesures au niveau système, en plus des mesures capturées par Container Insights, en utilisant les normes que vous avez définies pour Amazon EC2. Vous pouvez utiliser la même approche à partir duConfigurer State Manager et Distributor pour CloudWatch déploiement et configuration de l'agentde ce guide pour installer et configurer le CloudWatch Agent pour vos clusters Amazon EKS. Vous pouvez mettre à jour votre fichier de configuration CloudWatch spécifique à Amazon EKS pour inclure des mesures ainsi que la configuration de journal spécifique à Amazon EKS.

Le CloudWatch l'agent bénéficiant du support Prometheus peut automatiquement découvrir et gratter les métriques Prometheus depuischarges de travail et systèmes pris en charge et conteneurisés. Il les ingère comme CloudWatch journaux au format métrique intégré pour analyse avec CloudWatch Consigne Insights et crée automatiquement des mesures CloudWatch.

> **Important**
>
> Vous devez :déployer une version spécialiséedu CloudWatch Agent pour collecter des métriques Prometheus. C'est un agent séparé du CloudWatch Agent déployé pour Container Insights. Vous pouvez utiliser le pluginprometheus_jmxexemple d'application Java, qui inclut les fichiers de déploiement et de configuration pour le CloudWatch déploiement de l'agent et de l'espace Amazon EKS pour démontrer la découverte des mesures Prometheus. Pour de plus amples informations, veuillez consulterConfiguration d'un exemple d'application Java/JMX pour Amazon EKS et Kubernetesdans la documentation CloudWatch. Vous pouvez également configurer le CloudWatch pour capturer des mesures provenant d'autres cibles Prometheus exécutées dans votre cluster Amazon EKS.

Métriques d'application

Vous pouvez créer vos propres métriques personnalisées avec leMétriques intégrées CloudWatch. Pour ingérer des instructions de format de mesure intégrées, vous devez envoyer des entrées de format de mesure intégrées à un point de terminaison de format de mesure intégré. Le CloudWatch peut être configuré en tant qu'agentconteneur sidecar dans votre pod Amazon EKS. Le CloudWatch la configuration de l'agent est stockée sous forme de Kubernetes ConfigMap et lu par votre CloudWatch conteneur sidecar de l'agent pour démarrer le point de terminaison au format métrique intégré.

Vous pouvez également configurer votre application en tant que cible Prometheus et configurer l'agent CloudWatch, avec la prise en charge de Prometheus, pour découvrir, gratter et ingérer vos

métriques dans CloudWatch. Par exemple, vous pouvez utiliser leexportateur JMX open sourceavec vos applications Java pour exposer JMX Beans pour la consommation de Prometheus par le CloudWatch agent.

Si vous ne souhaitez pas utiliser le format de mesure intégré, vous pouvez également créer et mettre à jour des mesures CloudWatch en utilisantAWSAPIouAWS KIT DE DÉVELOPPEMENT LOGICIEL. Toutefois, ceci n'est pas recommandé, car elle mélange la surveillance et la logique d'application.

Mesures pour Amazon EKS sur Fargate

Fargate provisionne automatiquement les nœuds Amazon EKS pour exécuter vos pods Kubernetes afin que vous n'ayez pas besoin de surveiller et de collecter des mesures au niveau des nœuds. Toutefois, vous devez surveiller les mesures des espaces 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 :

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

Vous pouvez utiliser le pluginrouteur de bûches intégré pour Fargatepour envoyer des instructions de format de métrique intégrée à CloudWatch. Le routeur de journaux utilise Fluent Bit, qui possède un CloudWatch plugin pouvant être configuré pour prendre en charge les instructions de format de mesure intégrées.

Vous pouvez récupérer et capturer des mesures de niveau pod pour vos nœuds Fargate en déployant le serveur Prometheus dans votre cluster Amazon EKS pour collecter des mesures à partir de vos nœuds Fargate. Étant donné que Prometheus nécessite 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 basé sur Amazon EC2. Pour de plus amples informations, veuillez consulterSurveillance d'Amazon EKS surAWS Fargateutilisant Prometheus et Grafanasur leAWSBlog.

Surveillance Prometheus sur Amazon EKS

Amazon Managed Service for Prometheusfournit un système évolutif, sécurisé,AWSservice géré pour Prometheus open source. Vous pouvez utiliser Prometheus query Language (ProMQL) pour surveiller les performances des charges de travail conteneurisées sans gérer l'infrastructure sous-jacente pour l'ingestion, le stockage et l'interrogation de mesures opérationnelles. Vous pouvez collecter des mesures Prometheus à partir d'Amazon EKS et Amazon ECS en utilisantAWSDistro pour OpenTelemetry (ADOT)ou des serveurs Prometheus en tant qu'agents de collecte.

Surveillance de CloudWatch Container Insights pour Prometheusvous permet de configurer et d'utiliser le CloudWatch pour découvrir les mesures Prometheus à partir des charges de travail Amazon ECS, Amazon EKS et Kubernetes, et les ingérer sous forme de mesures CloudWatch. Cette solution est appropriée si CloudWatch est votre principale solution d'observabilité et de surveillance. Toutefois, la liste suivante décrit les cas d'utilisation dans lesquels Amazon Managed Service for Prometheus offre plus de flexibilité pour l'ingestion, le stockage et l'interrogation des mesures Prometheus :

- Amazon Managed Service for Prometheus vous permet d'utiliser des serveurs Prometheus existants déployés dans Amazon EKS ou Kubernetes autogéré et de les configurer pour écrire sur Amazon Managed Service for Prometheus au lieu d'un magasin de données configuré localement. Cela supprime la lourdeur indifférenciée de la gestion d'un magasin de données hautement disponible pour vos serveurs Prometheus et son infrastructure. Amazon Managed Service for Prometheus est un choix approprié lorsque vous disposez d'un déploiement Prometheus mature que vous souhaitez utiliser dans leAWScloud.
- Grafana prend directement en charge Prometheus comme source de données pour la visualisation. Si vous souhaitez utiliser Grafana avec Prometheus CloudWatch Tableaux de bord pour la surveillance de vos conteneurs, puis Amazon Managed Service for Prometheus pourrait 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'effectuer une analyse de vos mesures opérationnelles à l'aide de requêtes ProMQL. En revanche,le CloudWatch l'agent ingère des métriques Prometheus au format de métrique intégréedans CloudWatch Journaux qui aboutissent à CloudWatch métriques , Vous pouvez interroger les journaux de format de métrique intégrée à l'aide de CloudWatch Journaux Insights.
- Si vous n'avez pas l'intention d'utiliser CloudWatch pour la surveillance et la capture de mesures, 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 mesures de vos cibles Prometheus et configurer le serveur pourécriture à distance sur votre espace de travail Amazon Managed Service for Prometheus. Si vous utilisez Amazon Managed Grafana, vous pouvezintégrez directement Amazon Managed Grafana à votre source de données Amazon Managed Service for Prometheus à l'aide du plugin inclus. Étant donné que les données de mesure sont stockées dans Amazon Managed Service for Prometheus, il n'y a aucune dépendance pour déployer le CloudWatch agent ou obligation d'ingérer des données dans CloudWatch. Le CloudWatch est obligatoire pour la surveillance de Container Insights pour Prometheus.

Vous pouvez également utiliser ADOT Collector pour extraire une application instrumentée par Prometheus et envoyer les mesures à Amazon Managed Service for Prometheus. Pour plus d'informations sur ADOT Collector, consultez leAWSDistro pour OpenTelemetry.

Journalisation et statistiques pourAWS Lambda

Lambdaélimine le besoin de gérer et de surveiller les serveurs pour vos charges de travail et fonctionne automatiquement avec CloudWatchMétriques et CloudWatch Journalisation 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 Journaux, sans nécessiter 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 journaux 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 se trouve dans`/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`YYYY/MM/DD/[<FunctionVersion>]<InstanceId>`format. Le`InstanceId`est généré parAWSpour 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 Informations sur les journaux. 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 utilisermodule de journalisation Pythonpour 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 leAWSLambda Powertools pour Pythonboîte à outils pour les développeurs pour 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 un`LAMBDA_LOG_LEVEL`variable d'environnement qui définit le niveau de sortie du journal que vous pouvez récupérer à partir de votre code. L'exemple suivant tente de récupérer un`LAMBDA_LOG_LEVEL`variable d'environnement et utilisez la valeur pour définir la sortie de journalisation. Si la variable d'environnement n'est pas définie, sa valeur par défaut est`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 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 à unAWSservice de votre choix utilisant leAWSSDK.

Vous pouvez également utiliser les SDK pour les destinations de log en dehors duAWSIntégrez votre fonction Lambda dans le cloud pour envoyer directement des relevés de journal vers 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. Une surveillance et une 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 métrique intégré pour rendre la capture au niveau de l'application CloudWatch mesures plus faciles.

Métriques au niveau du système

Lambda s'intègre automatiquement à CloudWatch Métrique et fournit un ensemble demétriques 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.

Erreurs d'invocationempêcher 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 afin de détecter ces erreurs et d'avertir 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`Errors`La métrique capture et identifie les échecs d'exécution

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

CloudWatch fournitCloudWatch Informations sur Lambdaque 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`/aws/lambda-insights/`groupe de 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 métriques qui sont à la base de l'automatisation CloudWatch tableaux de bord. Nous vous recommandons d'activer Lambda Insights pour les tests de performance et les environnements de production. Les indicateurs supplémentaires créés par Lambda Insights incluent`memory_utilization`qui permet 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 dans CloudWatch en utilisant le format métrique intégré. Vous pouvez tirer partiAWS a fourni des bibliothèques pour le format métrique intégrépour créer et émettre des instructions au format métrique intégrées pour CloudWatch. Le Lambda intégré CloudWatch la fonction de journalisation est configurée pour traiter et extraire des instructions de format métrique intégrées correctement formatées.

Recherche et analyse des connexions CloudWatch

Une fois que vos journaux et statistiques 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) afin de faciliter la recherche et l'analyse de vos journaux. La plupart des charges de travail utilisent un ensemble deAWS 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 vosAWS charges de travail.

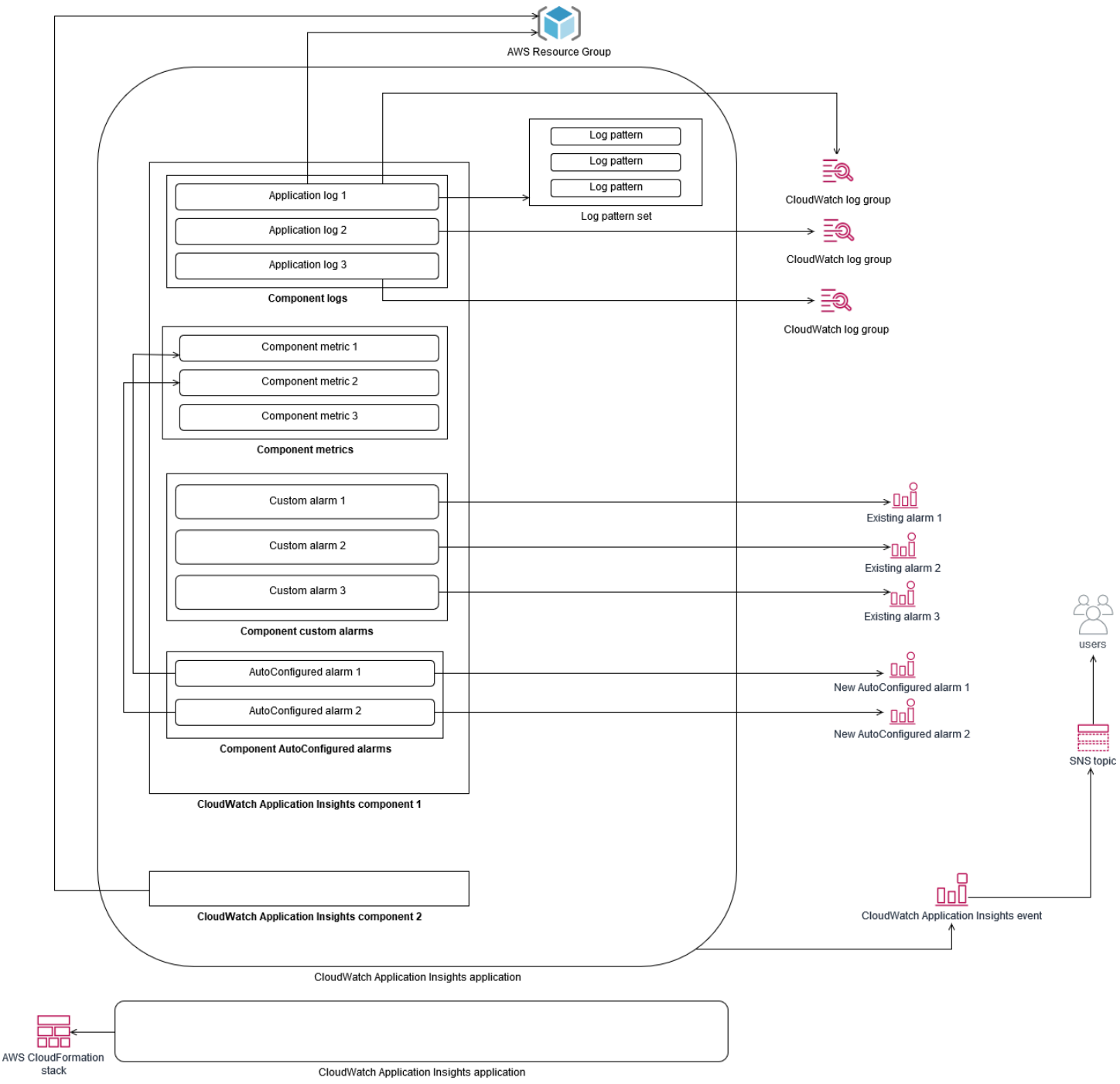
CloudWatch fournit plusieurs fonctionnalités pour aider à analyser les journaux et les indicateurs, telles que CloudWatch Application Insights pour définir et surveiller collectivement les métriques et les journaux d'une application sur différentesAWS ressources, la détection desCloudWatch anomalies pour détecter les anomalies pour votre des statistiques et des informations deCloudWatch journal pour rechercher et analyser de façon interactive vos données de journal dans CloudWatch Logs.

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 du système 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 la journalisation et la surveillance au niveau des applications. Il fournit également un cadre basé sur des composants qui aide les équipes à répartir les responsabilités en matière 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, indicateurs et alarmes.

Pour les journaux, vous définissez l'ensemble de modèles de log 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 en fonction d'expressions régulières, ainsi que d'une gravité faible, moyenne ou élevée lorsque le modèle est détecté. Pour les indicateurs, vous choisissez les indicateurs à surveiller pour chaque composant à partir d'une liste de métriques spécifiques au service et prises en charge. Pour les alarmes, CloudWatch Application Insights crée et configure automatiquement des alarmes standard ou de détection d'anomalies pour les indicateurs surveillés. CloudWatch Application Insights dispose de configurations automatiques pour les métriques et la capture de journaux pour les technologies décrites dans les journaux et les métriques prises en charge par CloudWatch Application Insights dans la CloudWatch documentation. Le diagramme suivant montre les relations entre les composants CloudWatch Application Insights et leurs configurations de journalisation et de surveillance. Chaque composant a défini ses propres journaux et métriques à surveiller à l'aide de CloudWatch journaux et de métriques.



Les instances EC2 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'instance EC2. Une commande Systems Manager est exécutée pour ajouter cette configuration à la configuration active de l'instance EC2. 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.

Réalisation d'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 dans 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 de requête de CloudWatch Logs Insights prend en charge des fonctions telles que l'agrégation avec des fonctions, par exemple sum (), avg (), count (), min () et max (), qui peuvent être utiles pour résoudre les problèmes de vos applications ou analyser les performances.

Si vous utilisez le format de métrique intégré pour créer des CloudWatch métriques, vous pouvez interroger vos journaux de format de métrique intégré afin de générer des métriques uniques 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 indicateurs spécifiques selon les besoins, au lieu de les capturer activement en tant que métriques personnalisées. Cela est particulièrement efficace pour les dimensions présentant une cardinalité élevée qui entraîneraient un grand nombre de mesures. CloudWatch Container Insights adopte également cette approche et collecte des données de performance détaillées, mais ne génère que CloudWatch des métriques pour un sous-ensemble de ces données.

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

```
{
```

```
"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 indicateurs capturés pour obtenir des informations supplémentaires. Par exemple, vous pouvez exécuter la requête suivante au niveau des 20 derniers espaces présentant des erreurs de page de mémoire :

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

Réalisation d'une analyse des journaux avec Amazon OpenSearch Service

CloudWatch s'intègre à Amazon OpenSearch Service en vous permettant de diffuser les données de CloudWatch journal des groupes de journaux vers un cluster Amazon OpenSearch Service de votre choix avec un filtre d'abonnement. Vous pouvez l'utiliser CloudWatch pour la capture et l'analyse des journaux et des indicateurs principaux, puis l'augmenter avec Amazon OpenSearch Service dans 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 terrain et aide à anonymiser les données dans les champs en fonction des autorisations des utilisateurs. C'est utile si vous souhaitez obtenir de l'aide pour résoudre les problèmes sans exposer de données sensibles.
- Regroupez et recherchez les journaux sur plusieurs comptes, régions et infrastructures : vous pouvez diffuser vos journaux depuis 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. Le streaming CloudWatch des journaux vers Amazon OpenSearch Service vous permet également de rechercher et d'analyser une application multirégionale dans un emplacement central.
- Expédiez et enrichissez les journaux directement à Amazon OpenSearch Service en utilisant ElasticSearch des agents : les composants de votre application et de votre pile technologique peuvent utiliser des systèmes d'exploitation qui ne sont pas pris en charge par l' CloudWatch agent. Vous souhaiterez peut-être également enrichir et transformer les données de journal avant qu'elles ne soient envoyées à 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 leur envoi à Amazon OpenSearch Service.
- La solution de gestion des opérations existante utilise uneElasticSearch 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 avec de nombreuses charges de travail 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 les CloudWatch journaux, vous pouvez utiliser les agents, les pilotes de journal et les bibliothèques pris en charge par Amazon OpenSearch Service (par exemple,

Fluent Bit, Fluentd, logstash et Open Distro pour ElasticSearch l'API) pour envoyer vos journaux directement à Amazon OpenSearch Service et les contourner CloudWatch. Cependant, vous devez également mettre en œuvre une solution pour capturer les journaux générés parAWS les services. CloudWatch Logs est la principale solution de capture de journaux pour de nombreuxAWS services et plusieurs services créent automatiquement de nouveaux groupes de journaux dans CloudWatch. Par exemple, Lambda crée un nouveau groupe de journaux pour chaque fonction Lambda. Vous pouvez configurer un filtre d'abonnement pour qu'un groupe de journaux diffuse ses journaux vers Amazon OpenSearch Service. Vous pouvez configurer manuellement un filtre d'abonnement pour chaque groupe de journaux individuel que vous souhaitez diffuser vers Amazon OpenSearch Service. Vous pouvez également déployer une solution qui inscrit automatiquement les nouveaux groupes de journaux aux ElasticSearch clusters. Vous pouvez diffuser les journaux vers un ElasticSearch cluster du même compte ou d'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 de vos comptes, régions et applications. Par exemple,AWS Control Tower configurez un compte Log Archive qui est utilisé pour la journalisation centralisée. Lorsqu'un nouveau compte est créé dansAWS Control Tower, sesAWS Config journauxAWS CloudTrail et sont transmis à un compartiment S3 de ce compte centralisé. La journalisation instrumentée parAWS Control Tower est destinée à la configuration, aux modifications et à la journalisation des audits.

Pour mettre en place une solution centralisée d'analyse 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 sur vos autres comptes pour diffuser les journaux vers le OpenSearch service Amazon centralisé. clusters.

Vous pouvez créer des clusters Amazon OpenSearch Service distincts pour gérer différentes applications ou couches de votre architecture cloud qui peuvent être distribuées 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. 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

La réalisation d'une analyse ponctuelle et automatisée de mesures importantes vous aide à détecter et à résoudre les problèmes avant qu'ils n'affectent vos charges de travail. CloudWatch facilite le diagramme et la comparaison de plusieurs mesures en utilisant plusieurs statistiques sur une période donnée. Vous pouvez utiliser CloudWatch pour effectuer une recherche sur toutes les mesures avec les valeurs de dimension requises pour trouver les mesures dont vous avez besoin pour votre analyse.

Nous vous recommandons de commencer votre approche de capture de mesures en incluant un ensemble initial de mesures et de dimensions à utiliser comme référence pour surveiller une charge de travail. Au fil du temps, la charge de travail arrive à maturité et vous pouvez ajouter des mesures et des dimensions supplémentaires pour vous aider à l'analyser et à la prendre en charge. Vos applications ou charges de travail peuvent utiliser plusieursAWSet possédant leurs propres mesures personnalisées, vous devez regrouper ces ressources sous un espace de noms pour les identifier plus facilement.

Vous devez également examiner comment les données de journalisation et de surveillance sont corrélées afin de pouvoir identifier rapidement les données de journalisation et de surveillance pertinentes pour diagnostiquer des problèmes spécifiques. Vous pouvez utiliserServiceLens CloudWatchpour corréler les traces, les mesures, les journaux et les alarmes pour diagnostiquer les problèmes. Vous devez également envisager d'inclure des dimensions supplémentaires dans les mesures et les identificateurs dans les journaux de vos charges de travail afin de vous aider à rechercher et à identifier rapidement les problèmes entre les systèmes et les services.

A l'aide de CloudWatch alarmes pour surveiller et alarmes

Vous pouvez utiliserAlarmes CloudWatchpour réduire la surveillance manuelle de vos charges de travail ou applications. Vous devez commencer par examiner les mesures que vous capturez pour chaque composant de charge de travail et déterminez les seuils appropriés pour chaque mesure. Assurez-vous d'identifier quels membres de l'équipe doivent être avertis lorsqu'un seuil est atteint. Vous devez établir et cibler des groupes de distribution plutôt que des membres individuels de l'équipe.

Les alarmes CloudWatch 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,AWSfournit le logicielAWSConnecteur de gestion des services pourServiceNowetCentre de

service Jirapour vous aider à configurer rapidement des intégrations. Cette approche est essentielle pour garantir que les alarmes déclenchées sont reconnues et alignées sur vos flux de travail opérationnels existants qui pourraient déjà être définis dans ces produits.

Vous pouvez également créer plusieurs alarmes pour la même mesure avec des seuils et des périodes d'évaluation différents, ce qui permet d'établir un processus d'escalade. Par exemple, si vous avez un`OrderQueueDepth`qui suit les commandes des clients, vous pouvez définir un seuil inférieur sur une courte période moyenne d'une minute qui notifie les membres de l'équipe d'application par e-mail ouSlack. Vous pouvez également définir une autre alarme pour la même mesure sur une période plus longue de 15 minutes au même seuil, et ces pages, courriels et avertir l'équipe d'application et le responsable de l'équipe d'application. Enfin, vous pouvez définir une troisième alarme pour un seuil moyen fort sur une période de 30 minutes qui notifie la haute direction et avertit tous les membres de l'équipe précédemment notifiés. La création de plusieurs alarmes vous aide à prendre différentes mesures pour différentes conditions. Vous pouvez commencer par un processus de notification simple, puis l'ajuster et l'améliorer au besoin.

A l'aide de CloudWatch détection d'anomalies pour surveiller et alarmer

Vous pouvez utiliserDétection d'anomalies CloudWatchsi vous n'êtes pas sûr des seuils à appliquer pour une mesure 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 mesures qui peuvent présenter des changements réguliers et prévisibles de l'activité, par exemple, les commandes d'achat quotidiennes pour une livraison le jour même augmentant avant une heure limite. La détection des anomalies permet de régler automatiquement les seuils et de réduire les fausses alarmes. Vous pouvez activer la détection des anomalies pour chaque mesure et statistique, et configurer CloudWatch pour alarmer en fonction des valeurs aberrantes.

Par exemple, vous pouvez activer la détection d'anomalies pour le`CPUUtilization`Metric et le paramètre`AVG`statistique sur une instance EC2. 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 d'alarme, similaire à la création de plusieurs alarmes standard avec des seuils différents.

Pour plus d'informations sur cette section, consultezCréation d'une alarme CloudWatch basée sur une détection d'anomaliedans le CloudWatch .

Une alarmante dans plusieurs comptes et régions

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 dans chaque compte et région dans lequel votre charge de travail est déployée. Vous pouvez simplifier et automatiser ce processus à l'aide d'un compte et d'une régionAWS CloudFormation StackSets et des modèles pour déployer des ressources applicatives avec les alarmes requises. TemplateVous pouvez configurer les actions d'alarme pour cibler une rubrique Amazon Simple Notification Service (Amazon SNS) commune, ce qui signifie que la même notification ou action de correction est utilisée quel que soit le compte ou la région.

Dans les environnements multi-comptes et multi-régions, 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 utilisantAWS CloudFormation StackSets et des mesures agrégées, telles que la moyenne`CPUUtilization`sur toutes les instances EC2.

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

Automation de la création d'alarmes avec les balises d'instance EC2

La création d'un ensemble d'alarmes standard pour vos instances EC2 peut prendre du temps, être incohérente et sujette à des erreurs. Vous pouvez accélérer le processus de création d'alarme en utilisant leAlarmes automatiques Amazon Cloudwatchpour créer automatiquement un ensemble standard d'alarmes CloudWatch pour vos instances EC2 et créer des alarmes personnalisées basées sur des balises d'instance EC2. La solution élimine la nécessité de créer manuellement des alarmes standard et peut être utile lors d'une migration à grande échelle d'instances EC2 utilisant des outils tels que CloudEndure. Vous pouvez également déployer cette solution avecAWS CloudFormation StackSets pour prendre en charge plusieurs comptes et régions. Pour de plus amples informations,

veuillez consulterUtiliser des balises pour créer et gérer Amazon CloudWatch alarmes pour instances Amazon EC2sur leAWSUn blog.

Surveillance de la disponibilité des applications et des services

CloudWatch vous aide à surveiller et à analyser les aspects de performance et 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 avecVérifications de l'état Amazon Route 53etCloudWatch Synthetics.

Vous pouvez utiliser les contrôles d'intégrité Route 53 lorsque vous souhaitez surveiller la connectivité à une page Web via HTTP ou HTTPS, ou la connectivité réseau via TCP vers un nom de système de noms de domaine (DNS) public ou une adresse IP. Les contrôles d'intégrité de Route 53 initient des connexions à partir des régions que vous spécifiez à intervalles de dix secondes ou de 30 secondes. Vous pouvez choisir plusieurs régions pour que le bilan de santé s'exécute, chaque vérification de santé s'exécute indépendamment et vous devez choisir au moins trois régions. Vous pouvez rechercher une sous-chaîne spécifique dans le corps de réponse d'une requête HTTP ou HTTPS si elle apparaît dans les 5 120 premiers octets de données renvoyées pour évaluation du contrôle de santé. Une requête HTTP ou HTTPS est considérée comme saine si elle retourne une réponse 2xx ou 3xx. Les contrôles de santé de Route 53 peuvent être utilisés pour créer un bilan de santé composite en vérifiant l'état de santé d'autres contrôles de santé. Vous pouvez le faire si vous disposez de plusieurs points de terminaison de service et que vous souhaitez effectuer la même notification lorsque l'un d'entre eux devient malsain. Si vous utilisez Route 53 pour DNS, vous pouvez configurer Route 53 surbasculement vers une autre entrée DNSsi un bilan de santé devient malsain. Pour chaque charge de travail critique, vous devez envisager de configurer des contrôles d'intégrité Route 53 pour les points de terminaison externes critiques pour les opérations normales. Les contrôles de santé Route 53 peuvent vous aider à éviter d'écrire une logique de basculement dans vos applications.

Les produits synthétiques CloudWatch vous permettent de définir un Canary comme script pour évaluer la santé et la disponibilité de vos charges de travail. Les scripts Canaris sont écrits dans Node.js ou Python et 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 de santé d'une série d'étapes, telles qu'un cas d'utilisation ou un point de terminaison avec des dépendances en aval. Création de scripts Canaris CloudWatch mesures qui incluent chaque étape exécutée afin que vous puissiez alarmer et mesurer

différentes étapes indépendamment. Bien que les Canaris nécessitent plus de planification et d'efforts pour développer que les contrôles de santé de la Route 53, ils vous offrent une approche de suivi et d'évaluation hautement personnalisable. Canaries prend également en charge les ressources privées exécutées dans votre cloud privé virtuel (VPC), ce qui les rend idéales pour la surveillance de la disponibilité lorsque vous n'avez pas d'adresse IP publique pour le point de terminaison. Vous pouvez également utiliser Canaries 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 vous disposez d'une charge de travail qui inclut des points de terminaison existants sur site.

Tracer les applications avecAWS X-Ray

Une demande via votre application peut consister en des appels vers des bases de données, des applications et des services Web exécutés sur des serveurs locaux, Amazon EC2, des conteneurs ou Lambda. En implémentant le suivi des applications, vous pouvez rapidement identifier la cause première des problèmes dans vos applications utilisant des composants et des services distribués. Vous pouvez utiliserAWS X-Raypour suivre les demandes de vos applications sur plusieurs composants. Exemples de X-Ray et visualise les demandes sur unGraphique de serviceslorsqu'ils circulent dans les composants de votre application et que chaque composant est représenté sous la forme d'un segment. X-Ray génère des identifiants de suivi afin que vous puissiez corréler une demande lorsqu'elle traverse plusieurs composants, ce qui vous aide à visualiser la demande de bout en bout. Vous pouvez encore améliorer cela en incluant des annotations et des métadonnées pour aider à rechercher et 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 passant des appels vers le service X-Ray. X-Ray fournit égalementAWSSDK pour plusieurs langues, y compris les clients instrumentés qui envoient automatiquement des données à X-Ray. Les kits SDK X-Ray fournissent des correctifs aux bibliothèques courantes utilisées pour passer des appels vers 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 relayer les données vers X-Ray. X-Ray crée des traces pour votre application qui capturent les données de performances des serveurs et des conteneurs exécutant le démon X-Ray qui a géré la demande. X-Ray instruit automatiquement vos appels versAWSservices, tels qu'Amazon DynamoDB, en tant que sous-segments grâce à la correction duAWSKIT SDK. X-Ray peut également s'intégrer automatiquement aux fonctions Lambda.

Si les composants de votre application passent des appels vers des services externes qui ne peuvent pas configurer et installer le démon X-Ray ou l'instrument du code, vous pouvez créersous-segments pour encapsuler les appels vers des services externes. Corrélations X-Ray CloudWatch journaux et mesures avec les traces de votre application si vous utilisez leKit SDK AWS X-Ray pour Java, ce qui signifie que vous pouvez analyser rapidement les métriques et les journaux associés pour les demandes.

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

Vous devez installer et exécuter le démon X-Ray sur les instances EC2 sur lesquelles vos composants d'application ou microservices s'exécutent. Vous pouvez utiliser unscript de données utilisateurpour déployer le démon X-Ray lorsque des instances EC2 sont provisionnées ou vous pouvez l'inclure dans le processus de génération de l'AMI si vous créez vos propres AMI. Cela peut être particulièrement utile lorsque les instances EC2 sont éphémères.

Vous devez utiliser State Manager pour vous assurer que le démon X-Ray est systématiquement installé sur vos instances EC2. Pour Amazon EC2Windows, vous pouvez utiliser le Systems ManagerAWS- Exécutez le document PowerShell Scriptpour exécuter leScript Windowsqui télécharge et installe l'agent X-Ray. Pour les instances EC2 sous Linux, vous pouvez utiliser leAWS-Document RunShellScript pour exécuter le script Linux quitélécharge et installe l'agent en tant que service.

Vous pouvez utiliser le Systems ManagerAWS- Exécutez un document Script distantpour exécuter le script dans un environnement multi-comptes. Vous devez créer un compartiment S3 accessible depuis tous vos comptes et nous vous recommandonscréation d'un compartiment S3 avec une stratégie de compartiment basée sur une organisationsi vous utilisezAWS Organizations. Vous téléchargez ensuite les scripts dans le compartiment S3, mais assurez-vous que le rôle IAM de vos instances EC2 est autorisé à accéder au compartiment et aux scripts.

Vous pouvez également configurer State Manager pour associer les scripts à des instances EC2 sur lesquelles l'agent X-Ray est installé. Étant donné que toutes vos instances EC2 peuvent ne pas nécessiter ou utiliser 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`InstallAWSXRayDaemonLinux`étiquettes.

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

Vous pouvez déployer leDémon X-Raycomme conteneur sidecar 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 sidecar avec liaison de conteneurs si vous utilisez Amazon ECS, ou le conteneur peut se connecter directement au conteneur sidecar sur localhost si vous utilisezMode réseau AWSVPC.

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

Configuration de Lambda pour suivre les demandes vers X-Ray

Votre application peut inclure des appels vers des fonctions Lambda. Vous n'avez pas besoin d'installer le démon X-Ray pour Lambda, car le processus de 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 leAWS Management Consoleet vérifiez leActive tracingdans la console X-Ray.

Pour effectuer une instrumentation complémentaire, vous pouvez regrouper le kit SDK X-Ray avec 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 passe vers d'autres systèmes. Examinez les clients fournis par la bibliothèque que vous avez choisie et vérifiez si le SDK peut automatiquement instrumenter le suivi pour la demande ou 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 que votre application appelle 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 instruisez votre application, assurez-vous de créer des annotations pour vous aider à identifier et à rechercher des demandes. Par exemple, votre application peut utiliser un identifiant pour les clients, tel que`customer id`, ou segmentez 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 segment ne dépasse pas 64 kilo-octets. Vous devez utiliser les annotations de manière sélective pour localiser les informations et utiliser l'objet de métadonnées pour fournir plus de contexte qui aide à résoudre les problèmes de la demande une fois qu'elle est localisée.

Configuration des règles d'échantillonnage X-Ray

Bitpersonnalisation des 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 kit SDK X-Ray le nombre de requêtes à enregistrer pour un ensemble de critères. Par défaut, le kit SDK X-Ray enregistrela première demande chaque seconde et cinq pour cent 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. 5 % 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 pour déterminer la valeur appropriée pour votre compte. Vos exigences peuvent varier dans les environnements de développement, de test, de test de performances et de production. Vous pouvez avoir des applications nécessitant 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 ligne de base et réévaluer régulièrement si la ligne de base répond à vos exigences.

Tableaux de bord et visualisations avec CloudWatch

Les tableaux de bord vous aident à vous concentrer rapidement sur les domaines préoccupants des applications et des charges de travail. CloudWatch fournit des tableaux de bord automatiques et vous pouvez également créer facilement des tableaux de bord utilisant CloudWatch métriques , CloudWatch Les tableaux de bord fournissent plus d'informations que de visualiser les mesures isolément, car ils vous aident à corréler plusieurs mesures 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 à la base de données peut vous aider à corréler les modifications des mesures de charge de travail entre plusieursAWSressources pendant que 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 par utiliser CloudWatch tableaux de bord automatiques, qui sontAWStableaux de bord de niveau de service préconfigurés avec des mesures spécifiques au service. Les tableaux de bord de service automatiques affichent toutes les normes CloudWatch Métriques pour le service. Les tableaux de bord automatiques représentent toutes les ressources utilisées pour chaque mesure de service et vous aident à identifier rapidement les ressources aberrantes sur votre compte. Cela peut vous aider à identifier les ressources à forte ou faible utilisation, ce qui peut vous aider à optimiser vos coûts.

Création de tableaux de bord entre services

Vous pouvez créer des tableaux de bord multiservices en affichant le tableau de bord automatique des niveaux de service d'unAWSservice et utilisation duAjouter au tableau de bordà partir de l'optionActionsmenu. Vous pouvez ensuite ajouter des mesures provenant d'autres tableaux de bord automatiques à votre nouveau tableau de bord et supprimer des mesures pour limiter le focus du tableau de bord. Vous devez également ajouter vos propres mesures personnalisées pour suivre les principales observations (par exemple, les commandes reçues ou les transactions par seconde). La création de votre propre tableau de bord inter-services personnalisé vous aide à vous concentrer sur les mesures les plus pertinentes pour votre charge de travail. Nous vous recommandons de créer des tableaux de bord inter-services au niveau du compte qui couvrent les mesures 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 d'opérations cloud, vous pouvez afficher le CloudWatch tableau de bord sur un grand écran de télévision en mode plein écran avec rafraîchissement 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 se concentrent sur des mesures et des 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 vos mesures personnalisées d'application ou de charge de travail et sont importantsAWSmesures de ressources qui influencent leurs performances.

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

Création de tableaux de bord entre régions et comptes

AWSles ressources sont principalement régionales et les mesures, les alarmes et les tableaux de bord sont spécifiques à la région dans laquelle les ressources sont déployées. Cela peut nécessiter de modifier les régions pour afficher les mesures, les tableaux de bord et les alarmes des charges de travail et des applications interrégions. Si vous séparez vos applications et vos charges de travail en plusieurs comptes, vous devrez peut-être également vous authentifier à nouveau et vous connecter à chaque compte. Cependant, CloudWatch prend en charge l'affichage des données entre comptes et inter-régions à partir d'un seul compte, ce qui signifie que vous pouvez afficher des mesures, des alarmes, des tableaux de bord et des 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 propriétaires d'équipes d'applications doivent créer des tableaux de bord pour des applications inter-régions spécifiques à un compte afin de surveiller efficacement les mesures clés dans un emplacement centralisé. Les tableaux de bord CloudWatch prennent automatiquement en charge les widgets inter-régions, ce qui signifie que vous pouvez créer un tableau de bord qui inclut des mesures provenant de plusieurs régions sans configuration supplémentaire.

Une exception importante est la CloudWatch Widget Logs Insights car les données de journal ne peuvent être affichées que pour le compte et la région auxquels vous êtes actuellement connecté. Vous pouvez créer des mesures spécifiques à une région à partir de vos journaux à l'aide de filtres de mesures. Ces mesures peuvent être affichées sur un tableau de bord inter-régions. Vous pouvez ensuite passer à la région spécifique lorsque vous devez analyser davantage ces journaux.

Les équipes opérationnelles doivent créer un tableau de bord centralisé qui surveille les mesures importantes entre comptes et interrégions. Par exemple, vous pouvez créer un tableau de bord inter-comptes qui inclut l'utilisation globale de l'UC dans chaque compte et région. Vous pouvez également utiliserMathématiques de métriquepour regrouper des données et des tableaux de bord dans plusieurs comptes et régions.

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

Vous pouvez utiliser les mathématiques des mesures pour vous aider à calculer des mesures dans des formats et des expressions pertinents pour 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 Amazon EBS fournissent le nombre de lectures (`VolumeReadOps`) et écrivez (`VolumeWriteOps`) des opérations effectuées sur une période spécifique.

Cependant,AWSfournit des directives sur les performances des volumes Amazon EBS dans les IOPS. Vous pouvez représenter un graphique et calculer les IOPS de votre volume Amazon EBS en mathématiques métriques en ajoutant le`VolumeReadOps`et`VolumeWriteOps`puis divisée par la période choisie pour ces mesures.

Dans cet exemple, nous résumons les IOPS de la période, puis nous divisons par la durée de la période pour obtenir les IOPS. Vous pouvez ensuite définir une alarme sur cette expression mathématique métrique pour vous alerter lorsque les IOPS de votre volume approchent de la capacité maximale de son type de volume. Pour plus d'informations et des exemples sur l'utilisation des maths de métriques pour surveiller les systèmes de fichiers Amazon Elastic File System (Amazon EFS) avec CloudWatch métriques, voirAmazon CloudWatch Metric Math simplifie la surveillance en temps quasi réel de vos systèmes de fichiers Amazon EFS et bien plus encoresur leAWSBlog.

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

CloudWatch Container Insights crée des tableaux de bord dynamiques et automatiques pour les charges de travail de conteneurs exécutées sur Amazon ECS et Amazon EKS. Vous devez permettre à Container Insights d'avoir une observabilité des informations de CPU, de mémoire, de disque, de réseau et de diagnostic telles que les échecs de redémarrage du conteneur. Container Insights génère des tableaux de bord dynamiques que vous pouvez filtrer rapidement au niveau du cluster, de l'instance ou du nœud de conteneur, du service, de la tâche, de l'espace et du conteneur individuel. Container Insightsest configuré au niveau du cluster et du nœud ou de l'instance de conteneurselon leAWSservice.

Similaire à 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 de niveau système, notamment le temps de CPU, la mémoire, le disque et le réseau. Elle collecte, agrège et résume également des informations de diagnostic telles que des démarrages à froid et des arrêts de rôle de travail 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 de X-Ray et à une carte de service pour visualiser vos charges de travail de conteneur. Ils utilisent tous les deux le CloudWatch format de métrique intégrée à capturer CloudWatch Métriques et journaux de performance.

Vous pouvez créer un objet partagé CloudWatch tableau de bord pour votre charge de travail qui utilise les mesures capturées par Container Insights et Lambda Insights. Vous pouvez le faire en filtrant et en affichant le tableau de bord automatique à l'aide de CloudWatch Container Insights, puis choisir leAjouter au tableau de bordqui vous permet d'ajouter les mesures affichées à un tableau de bord CloudWatch standard. Vous pouvez ensuite supprimer ou personnaliser les mesures et ajouter d'autres mesures pour représenter correctement votre charge de travail.

Intégration de CloudWatch àAWSservices

AWSfournit de nombreux services qui incluent des options de configuration supplémentaires pour la journalisation et les mesures. Ces services vous permettent souvent de configurer CloudWatch Journaux pour la sortie du journal et CloudWatch mesures pour la sortie des mesures. L'infrastructure sous-jacente utilisée pour fournir ces services est gérée parAWSetinaccessible, mais vous pouvez utiliser les options de journalisation et de mesure de vos services provisionnés pour obtenir des informations supplémentaires et résoudre les problèmes. Par exemple, vous pouvez publierJournaux de flux VPC vers CloudWatch, ou vous pouvez également Configuration des instances Amazon Relational Database Service (Amazon RDS) pour publier des journaux vers CloudWatch.

MostAWSJournaux aux appels d'API avecIntégration de àAWS CloudTrail. CloudTrail également prend en charge l'intégration avec . CloudWatch JournauxCela signifie que vous pouvez rechercher et analyser l'activité dansAWSServices . Vous pouvez également utiliser Amazon CloudWatch Événements ou Amazon EventBridge pour créer et configurer l'automatisation et les notifications avec CloudWatch Règles d'événements pour des actions spécifiques exécutées dansAWSServices . Certains servicesIntégration directe d'avec CloudWatch Événements d'et EventBridge. Vous pouvez également créer des événements livrés via CloudTrail.

Amazon Managed Grafana pour le tableau de bord et la visualisation

Amazon Managed Grafanapeut être utilisé pour observer et visualiser votreAWSapplications. Amazon Managed Grafana vous permet de visualiser et d'analyser vos données opérationnelles à grande échelle. Grafanaest une plateforme d'analyse open source qui vous permet d'interroger, de visualiser, d'émettre des alertes et de comprendre vos métriques, quel que soit l'endroit où elles sont stockées. Amazon Managed Grafana est particulièrement utile si votre organisation utilise déjà Grafana pour visualiser les charges de travail existantes et si vous souhaitez étendre la couverture àAWSapplications. Vous pouvez utiliser Amazon Managed Grafana avec CloudWatch paren l'ajoutant en tant que source de données, ce qui signifie que vous pouvez créer des visualisations à l'aide de CloudWatchmétriques , Amazon Managed GrafanaAWS Organizationset vous pouvez centraliser les tableaux de bord à l'aide de CloudWatch Métriques de plusieurs comptes et régions.

Le tableau suivant présente les avantages et les points à prendre en compte pour utiliser Amazon Managed Grafana au lieu de CloudWatch pour le tableau de bord Une approche hybride peut convenir 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 Grafana open source	Amazon Managed Grafana vous aide à créer des visualisations et des tableaux de bord à partir de nombreuses sources de données différentes, notamment CloudWatch métriques , Amazon Managed Grafana inclut un certain nombre de sources de données intégrées qui couvrentAWSservices, logiciels open source et logiciels COTS. Pour de plus amples informati ons à ce sujet, consultezSources de données intégréesdans la documentation Amazon Managed Grafana. Vous pouvez également ajouter la prise en charge de sources de données supplémentaires en mettant à niveau votre espace de travail versGrafana. Grafana prend également en chargeextension

	s de source de donnéesqui vous permetten t de communiquer avec différents systèmes externes. CloudWatchles tableaux de bord nécessitent un CloudWatch Métriques ou CloudWatch Requête Logs Insights pour les données à afficher sur un CloudWatch Tableau de bord.
Gérez l'accès à votre solution de tableau de bord séparément de votreAWSaccéder à un compte	Amazon Managed Grafana nécessite l'utilisa tion deAWS IAM Identity Center(IAM Identity Center) etAWS Organizationspour l'authent ification et l'autorisation. Cela vous permet d'authentifier les utilisateurs auprès de Grafana en utilisant la fédération d'identités que vous utilisez peut-être déjà avec IAM Identity Center ouAWS Organizations. Toutefois, si vous n'utilisez pas IAM Identity Center ouAWS Organizations, puis il est configuré dans le cadre du processus de configuration Amazon Managed Grafana. Cela peut poser problème si votre entreprise a limité l'utilisation d'IAM Identity Center ouAWS Organizations.

Ingérez et accédez aux données de plusieurs comptes et régions avecAWS Organizat ionsintégration	Amazon Managed Grafana s'intègre àAWS Organizationspour vous permettre de lire les donnéesAWSdes sources telles que CloudWatch et Amazon OpenSearch Service sur tous vos comptes. Cela permet de créer des tableaux de bord qui affichent des visualisa tions à partir des données de vos comptes. Pour activer automatiquement l'accès aux données surAWS Organizations, vous devez configurer votre espace de travail Amazon Managed Grafana dans laAWS Organizationscompte de gestion Ceci n'est pas recommandé en raison deAWS Organizat ionsBonnes pratiques relatives au compte de gestion. En revanche, CloudWatch également prend en charge les tableaux de bord entre régions et comptes pour CloudWatch indicateu rs.
Utilisez les widgets de visualisation avancés et les définitions Grafana disponibles dans la communauté open source	Grafana propose 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 en fonction de vos besoins.
Utiliser 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 aux exigences des cas d'utilisation plus avancés, ainsi qu'aux configurations de sécurité avancées. Les fonctionnalités avancées peuvent nécessiter que vos équipes développe nt 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 mon CloudWatch fichiers de configuration ?

Le CloudWatch agent pour Amazon EC2 peut appliquer plusieurs fichiers de configuration stockés dans le CloudWatch répertoire de configuration. Idéalement, vous devez stocker votre configuration CloudWatch sous la forme d'un ensemble de fichiers, car vous pouvez contrôler la version et les utiliser à nouveau sur plusieurs comptes et environnements. Pour de plus amples informations à ce sujet, veuillez consulter leGestion des CloudWatch configurationsde ce guide. Vous pouvez également stocker vos fichiers de configuration dans un référentiel sur GitHub et automatisez la récupération des fichiers de configuration lorsqu'une nouvelle instance EC2 est provisionnée.

Comment puis-je 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 configurez l' CloudWatch alarme pour avertir le sujet SNS lorsqu'une alarme est déclenchée. Votre système intégré reçoit le message SNS et peut créer un ticket à l'aide des API ou des kits SDK de vos systèmes de gestion des services.

Comment utiliser ? CloudWatch pour capturer des fichiers journaux dans mes conteneurs ?

Les tâches Amazon ECS et les espaces Amazon EKS peuvent être configurés pour envoyer automatiquement la sortie 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 vers STDOUT et STDERR. Cela est également abordé dans leManifeste de l'application à douze facteurs.

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

ECS à l'endroit où votre application écrira ses fichiers lot et utiliser un conteneur sidecar pour Fluentd ou Fluent Bit pour envoyer les journaux à CloudWatch. Vous devez envisager de lier symboliquement un fichier journal spécifique de votre conteneur à`/dev/stdout`et`/dev/stderr`. Pour de plus amples informations à ce sujet, veuillez consulter.Afficher les journaux d'un conteneur ou d'un servicedans la documentation Docker.

Comment puis-je surveiller les problèmes de santé pourAWSservices ?

Vous pouvez utiliser le pluginAWS Health Dashboardpour surveillerAWSévénements d'état. Vous pouvez également vous référer à l'outils de santé AWS GitHub référentiel pour exemples de solutions d'automatisation liées àAWSévénements d'état.

Comment créer une personnalisation CloudWatch mesure lorsqu'aucun support d'agent n'existe ?

Vous pouvez utiliser le format de métrique intégrée pour ingérer des métriques dans CloudWatch. Vous pouvez également utiliserAWSSDK (par exemple,put_metric_data),AWS CLI(par exemple,put-metric-data), ouAWSAPI (par exemple,PutMetricData) pour créer des métriques personnalisées. Vous devez réfléchir à la façon dont une logique personnalisée sera maintenue à long terme. Une approche consisterait à utiliser Lambda avec la prise en charge intégrée du format de mesure intégré pour créer vos mesures, ainsi qu'un CloudWatch Événements d'événementsrègle de planificationpour établir la période de la mesure.

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

Vous devez vous référer aux conseils fournis par le fournisseur de logiciels ou de services pour l'intégration avecAWS. Vous pouvez peut-être utiliser un logiciel d'agent, un SDK ou une API fournie pour envoyer des journaux et des mesures 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 l'AWSKit SDK et CloudWatch Consigne les filtres d'abonnement avec Lambda et Kinesis Data Streams pour créer des processeurs de journaux et des expéditeurs personnalisés. Enfin, vous devez également réfléchir à la façon dont vous allez intégrer le logiciel si vous utilisez plusieurs comptes et régions.

Ressources

Introduction

- AWSWell-Architected Tool

Résultats commerciaux ciblés

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

Planification de votre CloudWatch déploiement

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

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

- Dimensions de métriques Amazon EC2

- Instances à capacité extensible
- CloudWatch ensembles de métriques prédéfinis de l'agent
- Collecter des métriques de processus avec le plugin procstat
- Configuration de l' CloudWatch agent pour Procstat
- Activer ou désactiver la surveillance détaillée pour vos instances
- Ingestion des journaux de cardinalité élevée et génération des métriques avec un format de métrique CloudWatch intégrée
- Utilisation des groupes de journaux et des flux de journaux
- Répertorier CloudWatch les métriques disponibles pour vos instances
- PutLogEvents
- Récupération de métriques personnalisées avec collectd
- Récupération de métriques personnalisées avec StatsD

CloudWatch approches d'installation d'agents pour Amazon EC2 et serveurs locaux

- Créer un rôle de service IAM pour un environnement hybride
- Création d'une activation d'instance gérée pour un environnement hybride
- Création des rôles et utilisateurs IAM à utiliser avec l' CloudWatch agent
- Télécharger et configurer l' CloudWatch agent à l'aide de la ligne de commande
- Comment puis-je configurer les serveurs locaux qui utilisent l'agent Systems Manager et l' CloudWatchagent unifié pour n'utiliser que des informations d'identification temporaires ?
- Prérequis pour les opérations sur les ensembles de piles
- Utilisation d'instances ponctuelles

Journalisation et surveillance sur Amazon ECS

- amazon-cloudwatch-logs-for-fluent-bit
- CloudWatch Métriques Amazon ECS
- Métriques de Container Insights pour Amazon ECS

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

Journalisation et surveillance sur 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
- Surveillance des métriques Prometheus Container Insights
- Contrôlez les métriques du plan avec Prometheus
- Déploiement du tableau de bord Kubernetes (interface utilisateur web)
- Exploitation forestière 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 des métriques Prometheus
- Installation du serveur de métriques Kubernetes
- kubernetes/tableau de bord
- Horizontal Pod Autoscaler
- Composants du plan de contrôle Kubernetes

- Pods Kubernetes
- Support 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
- prométhéuse/jmx_exporter
- Récupération de sources Prometheus supplémentaires et importation de ces métriques
- Nœuds autogérés
- Envoyer des journaux à CloudWatch Logs
- Configurer FluentD pour l'envoi DaemonSet de CloudWatch journaux à Logs
- Configuration d'un exemple d'application Java/JMX pour Amazon EKS et Kubernetes
- Didacticiel pour l'ajout d'une nouvelle cible de récupération Prometheus : métriques du serveur d'API Prometheus
- Autodétartreur à pod vertical

Journalisation et statistiques pourAWS Lambda

- Erreurs d'invocation Lambda
- journalisation : fonction de journalisation pour Python
- Utilisation des bibliothèques clientes pour générer des journaux de format de métrique intégrée
- Utilisation des métriques de 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
- AWSConnecteur de gestion des services pour Jira Service Management
- AWSConnecteur de gestion des services pour ServiceNow

Surveillance de la disponibilité des applications et des services

- Configuration du basculement DNS

Suivi des applications avecAWS 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 démon X-Ray sur Amazon EC2
- Envoi de données de suivi à X-Ray
- Graphique de service en 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 maths de métriques

CloudWatch intégration avec lesAWS services

- Intégrations et services pris en charge par AWS CloudTrail
- CloudWatch Événements et exemples d'événements provenant de services pris en charge
- Événements organisés via CloudTrail
- Surveillance des fichiers CloudTrail journaux avec CloudWatch Logs

- Publication des journaux du moteur de base de données dans CloudWatch Logs
- Publication des journaux de flux dans CloudWatch Logs

Amazon Managed Grafana pour le tableau de bord et la visualisation

- Bonnes pratiques relatives au compte de gestion dansAWS Organizations
- Sources de données intégrées pour Amazon Managed Grafana
- Tableaux de bord entre comptes et régions dans CloudWatch
- Plugins Grafana

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Si vous souhaitez être informé des future mises à jour, vous pouvez vous abonner à un fil RSS.

Modification	Description	Date
Informations de journalisation mises à jour	Mise à jour de la section concernant la journalisation deAWS Lambda.	17 avril 2023
Informations de configuration mises à jour	Mise à jour et renommée de la section sur la création et le stockage de CloudWatch configurations.	9 février 2023
Informations de mesure mises à jour	Mise à jour des informations relatives aux métriques des applications personnalisées dans la section Métriques pour Amazon ECS.	31 janvier 2023
Notices d'aperçu supprimées	Amazon Managed Grafana est en disponibilité.	25 mai 2022
Section supprimée	CloudWatch SDK Metrics n'est plus pris 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 Amazon Aurora Édition compatible avec 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 in the Cloud. AWS
- 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 sur site vers Oracle sur une instance EC2 dans le 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. Ce scénario de migration est spécifique à VMware Cloud on AWS, qui prend en charge la compatibilité des machines virtuelles (VM) et la portabilité de la charge de travail entre votre environnement sur site et AWS. Vous pouvez utiliser les technologies VMware Cloud Foundation à partir de vos centres de données sur site lorsque vous migrez votre infrastructure vers VMware Cloud on AWS. Exemple : déplacez l'hyperviseur hébergeant votre base de données Oracle vers VMware Cloud on. 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 la synchronisation des bases de données source et cible est maintenue, mais seule la base de données source gère les transactions provenant de la connexion d'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 la façon dont les AIOps sont utilisées dans la stratégie de migration AWS , veuillez consulter 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, c'est 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.

CCoE

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 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 articles du CCoE sur le blog AWS Cloud Enterprise Strategy.

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 le 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 mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant un CCoE ou en établissant 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 on the AWS Cloud Enterprise Strategy blog. 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 ou AWS CodeCommit. 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, AWS

Panorama propose des appareils qui ajoutent des CV aux réseaux de caméras locaux, et Amazon SageMaker 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 source, de génération, de test, intermédiaire 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

Consultez la section 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.

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.

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 pipeline CI/CD, 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.

épopée

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 la 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.

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 via 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.

G

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.

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 d'organisation (UO). 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 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 de l'historien

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.

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.

IIoT

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 de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et 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

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, veuillez consulter Building an industrial Internet of Things (IIoT) digital transformation strategy.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau entre les VPC (identiques ou Régions AWS différents), Internet et les réseaux sur site. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et 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, veuillez consulter Machine learning model interpretability with 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.

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.

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 la 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 qui AWS gère 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 connus sous le nom de 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 au fur et à mesure de son fonctionnement. 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/abonnement, pour les appareils IoT aux ressources limitées.

microservice

Petit service indépendant qui communique via des API bien définies 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 à l'aide d'API légères. 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 les opérations, les analystes commerciaux et les propriétaires, les ingénieurs de migration, les développeurs et les DevOps 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 AWS avec le service de migration d'applications.

Évaluation du portefeuille de migration (MPA)

Un 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

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, veuillez consulter Evaluating modernization readiness for applications in the 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.

OU

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 de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et 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 informations de contact.

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 capable d'effectuer AWS des actions et d'accéder à des 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 de l'ingénierie des systèmes qui prend en compte la confidentialité tout au long du processus d'ingénierie.

zones hébergées privées

Conteneur qui contient des informations concernant la façon dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines dans un ou plusieurs VPC. 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.

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.

publier/souscrire (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).

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. Cela permet de déterminer ce qui est considéré comme une perte de données acceptable entre le dernier point de restauration 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

Un ensemble de AWS ressources dans une zone géographique. Chacune Région AWS est isolée et indépendante 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 la section 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.

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 d' 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, consultez la section Secret dans la documentation de Secrets Manager.

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 instance Amazon EC2 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 propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. Les SCP définissent des barrières de protection ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser les SCP comme listes d'autorisation ou de refus, pour indiquer 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.

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

Hub de transit de réseau que vous pouvez utiliser pour relier vos VPC et vos réseaux 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

Connexion entre deux VPC qui vous permet d'acheminer le trafic à l'aide d'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

Consultez le cadre de qualification des charges de travail AWS.

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 de type « 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.

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.