Pratiques éprouvées pour développer une stratégie multicloud

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Pratiques éprouvées pour développer une stratégie multicloud

Table of Contents

Pratiques éprouvées pour développer une stratégie multicloud

Tom Godden et Ellie Tamari, Amazon Web Services

Septembre 2025 (historique du document)

Organisations d'aujourd'hui sont confrontées à des messages contradictoires concernant l'adoption du multicloud. Certains le déconseillent totalement, tandis que d'autres affirment que tout le monde passe à un environnement multicloud. La réalité se situe entre ces deux extrêmes : des raisons légitimes existent à la fois pour et contre les stratégies multicloud, et le succès dépend de l'équilibre entre la valeur commerciale potentielle et la complexité et les risques inhérents.

Chez AWS, notre engagement en faveur de l'interopérabilité est l'une des principales raisons pour lesquelles de nombreux clients choisissent notre plateforme. Nous croyons qu'il est important de vous donner la liberté d'innover quelle que soit votre charge de travail et de vous donner les moyens de choisir la technologie qui répond le mieux à vos besoins. Chez AWS, nous avons joué un rôle de premier plan dans le développement de solutions qui vous permettent de créer et de déployer des applications dans n'importe quel environnement. Cette approche centrée sur le client est fondamentale pour la AWS Cloud confiance de millions de clients dans le monde entier.

Nous sommes conscients que les clients ont besoin de plateformes cloud qui fonctionnent parfaitement avec les outils existants et les choix technologiques futurs. Vous ne devriez pas avoir à tout reconstruire lorsque vous ajoutez des fonctionnalités d'un autre fournisseur. Votre cloud doit vous aider à connecter, sécuriser et gérer les charges de travail dans tous les environnements sans vous obliger à devenir un expert de chaque plateforme. AWS intègre des points de connexion directement dans ses services pour vous aider à fonctionner efficacement, que votre stratégie soit d'utiliser AWS exclusivement ou de suivre une approche multicloud sélective.

Nous sommes conscients que chaque entreprise a des exigences commerciales uniques qui orientent ses décisions en matière de stratégie cloud. Que vous exécutiez des charges de travail principalement sur AWS, sur plusieurs clouds ou que vous les utilisiez dans AWS le cadre d'une architecture multicloud plus large, nous nous engageons à vous aider à réussir. AWS fournit l'ensemble des outils et des fonctionnalités nécessaires pour vous aider à créer, à migrer et à exploiter plus facilement et plus rapidement, quel que soit le lieu où se trouvent vos charges de travail. AWS les outils simplifient la gestion entre les fournisseurs tout en maximisant les performances et la valeur de vos investissements dans le cloud.

Ce paper met l'accent sur les principes éprouvés pour réussir une stratégie multicloud, notamment quand et où une approche multicloud est judicieuse et comment AWS aider les entreprises à réussir leurs stratégies multicloud. Il fournit des conseils prescriptifs pour aider les dirigeants à faire des choix stratégiques et décisionnels éclairés liés à l'adoption du multicloud. Ce paper ne propose pas de discussion technique approfondie sur les implémentations multicloud. Pour le soutien technique à la mise en œuvre et l'assistance à relever vos défis spécifiques, nous vous recommandons de travailler avec votre architecte de AWS solutions.

Ce paper présente neuf principes éprouvés du succès du multicloud sur la base de nos expériences avec les AWS entreprises clientes. Chaque principe aborde un aspect essentiel de la stratégie multicloud, de l'alignement des objectifs commerciaux à la mise en œuvre de la sécurité. En appliquant ces principes, les entreprises peuvent gérer la complexité du multicloud en toute confiance.

- Principe 1. Alignez les objectifs multicloud avec votre stratégie
- Principe 2. Soyez conscient des idées reçues concernant le multicloud
- Principe 3. Disposer d'une stratégie et d'une gouvernance claires pour le soutenir
- Principe 4. Ne répartissez pas les charges de travail contiguës entre les clouds
- Principe 5. Disposer d'une stratégie d'intégration à plus long terme
- Principe 6. Utiliser les contenants de façon stratégique
- Principe 7. Avoir un seul CCo E, mais se spécialiser dans ce domaine
- Principe 8. Assurez-vous que la sécurité est toujours une priorité absolue
- Principe 9. Adoptez une approche 80/20 en matière de distribution équitable

Principe 1. Alignez les objectifs multicloud avec votre stratégie

Les recherches menées par Gartner et les tendances du secteur montrent que les entreprises adoptent de plus en plus des approches multicloud pour répondre à des besoins commerciaux spécifiques. Les scénarios suivants montrent dans quels cas une infrastructure multicloud peut être stratégiquement avantageuse.

Fusions et acquisitions

Les fusions et acquisitions (M&A) permettent de prendre des décisions immédiates en matière de stratégie cloud. Bien que l'exploitation de plusieurs clouds puisse augmenter les coûts et la complexité, une consolidation rapide peut retarder la valeur de l'intégration et perturber les opérations commerciales. Vos décisions relatives au cloud deviennent essentielles pour tirer parti des avantages des fusions et acquisitions.

La planification de l'intégration doit tenir compte de l'ensemble du paysage technologique. Chaque charge de travail doit être évaluée dans le contexte de votre calendrier d'intégration et de vos priorités commerciales.

Nos conseils :

- Développez une stratégie de consolidation axée sur l'entreprise qui équilibre les besoins d'intégration immédiats avec l'efficacité opérationnelle à long terme. Maintenez plusieurs clouds dans un premier temps dans des circonstances où une consolidation précipitée pourrait perturber les opérations commerciales critiques ou retarder la concrétisation de la valeur des fusions et acquisitions.
- Créez des critères de placement de charge de travail clairs qui correspondent à votre calendrier d'intégration. Priorisez les applications génératrices de revenus et les principaux processus métier tout en tenant compte des dépendances techniques et des exigences opérationnelles.

Désir de tirer parti des capacités différenciées à long terme d'un autre CSP

La peur de passer à côté d'une occasion pousse certaines entreprises à vouloir profiter de tous les clouds. Les décisions relatives au placement de la charge de travail concernent l'ensemble de

l'organisation, des équipes d'ingénierie aux opérations financières en passant par les opérations de sécurité.

Organisations doivent donc examiner les raisons pour lesquelles elles optent pour de multiples clouds. Certains soutiennent que chaque charge de travail doit être confiée au fournisseur de services cloud (CSP) qui répond le mieux à ses besoins. Cependant, l'optimisation individuelle de la charge de travail doit être équilibrée par rapport à l'impact organisationnel plus large. Chaque fournisseur de cloud supplémentaire risque d'accroître la complexité opérationnelle, de créer de nouveaux besoins en talents et d'introduire des considérations de sécurité qui affectent l'ensemble de l'organisation technologique.

Nos conseils :

- Adoptez une approche 80/20 : sélectionnez un fournisseur principal pour la plupart des charges de travail et considérez des fournisseurs supplémentaires uniquement pour des cas d'utilisation spécifiques et de grande valeur. Cette stratégie maximise l'efficacité et la rétention des talents tout en réduisant la complexité.
- Tenez compte du coût total de l'exploitation dans les clouds. Incluez les outils de sécurité, les produits de gouvernance, les systèmes de gestion financière et les frais opérationnels dans votre analyse.
- Évaluez les dépendances et les interactions de chaque charge de travail. Les charges de travail fonctionnent rarement de manière isolée ; elles partagent les données, les contrôles de sécurité et les processus opérationnels.
- Procédez à une analyse prix-performance approfondie de tous les fournisseurs. Comparez non seulement les coûts directs, mais également les frais généraux liés à la gestion de plusieurs environnements.

Multicloud dans la société holding et cloud principal dans la société d'exploitation ou le secteur d'activité

Les sociétés de capital-investissement et les sociétés de portefeuille sont confrontées à des considérations uniques en matière de stratégie cloud. Les sociétés de leur portefeuille appliquent souvent des stratégies cloud indépendantes, résultant souvent d'activités de fusions-acquisitions passées. Cette structure réduit la complexité généralement associée aux opérations multicloud, car chaque unité commerciale fonctionne de manière indépendante. Cependant, cette indépendance

peut limiter les possibilités de tirer parti des remises sur volume et des incitations à l'achat à l'échelle de l'entreprise.

L'efficacité de la stratégie cloud au niveau de la société holding dépend de l'autonomie des sociétés du portefeuille et de leurs besoins technologiques individuels. Bien que la consolidation puisse créer un effet de levier d'achat, elle peut entrer en conflit avec le modèle d'exploitation indépendant typique des sociétés de portefeuille et des portefeuilles de capital-investissement.

Nos conseils :

- Comprenez les structures de réduction du volume des CSP. Chaque fournisseur propose des mécanismes permettant d'ajouter ou de supprimer des filiales dans les contrats d'entreprise et de scinder des unités commerciales en entités distinctes. Il s'agit de décisions bidirectionnelles.
- Planifiez soigneusement vos engagements d'achat dans le cloud. Contactez rapidement l'équipe chargée des comptes de votre CSP ou contactez un spécialiste AWS Partner des opérations AWS cloud pour obtenir de l'aide.
- Trouvez le juste équilibre entre indépendance et efficacité. Envisagez des services partagés ou des contrats d'achat qui profitent aux sociétés du portefeuille sans pour autant limiter leurs activités.
- Concentrez-vous d'abord sur les objectifs commerciaux. Développez des stratégies technologiques qui soutiennent votre modèle d'exploitation plutôt que de poursuivre une stratégie multicloud en elle-même.
- Évaluez les stratégies cloud sous l'angle de la gestion de portefeuille. Réfléchissez à l'impact des choix du cloud sur les cessions potentielles ou les futures acquisitions.

Principe 2. Soyez conscient des idées reçues concernant le multicloud

Lorsque vous élaborez votre stratégie multicloud, évitez les idées reçues fréquemment évoquées dans les sections suivantes.

Tout le monde adopte des stratégies multicloud

Les sociétés de conseil et les entreprises de médias brossent un tableau complexe de l'adoption du multicloud. Les études montrent un grand intérêt pour les approches multicloud, mais les modèles de dépenses racontent souvent une autre histoire. Dans la pratique, de nombreuses entreprises maintiennent soit des environnements cloud uniques, soit des relations claires avec le primary/secondary CSP. Ce décalage met en évidence l'importance de regarder au-delà des gros titres et de se concentrer plutôt sur les besoins spécifiques de votre organisation.

Nos conseils :

- Prenez des décisions relatives au cloud en fonction des besoins spécifiques de votre entreprise plutôt que de suivre les tendances du secteur. Concentrez-vous sur les coûts et les risques mesurables pour votre organisation.
- Examinez les cas d'utilisation du multicloud dans le contexte de votre secteur d'activité. Les stratégies cloud qui fonctionnent pour les entreprises de technologie grand public peuvent ne pas se traduire par des environnements de services financiers, de fabrication ou de jeu.
- Tenez compte de la gravité des données comme un facteur essentiel dans les décisions relatives au placement de la charge de travail. L'emplacement et le mouvement des données déterminent souvent l'architecture cloud la plus efficace.
- Ne vous limitez pas aux statistiques d'adoption pour comprendre les habitudes de dépenses. Les taux élevés d'adoption du multicloud signalés masquent souvent les habitudes de dépenses réelles.
- Évaluez les contraintes techniques avant de vous engager dans un environnement multicloud. Certaines charges de travail sont plus performantes lorsque leurs composants restent dans un environnement cloud unique.

Le multicloud réduit le risque de dépendance vis-à-vis d'un fournisseur

La flexibilité des fournisseurs est une considération légitime dans le développement d'une stratégie cloud. Organisations attachent de l'importance à la capacité d'adapter leurs choix technologiques en fonction de l'évolution de leurs besoins. Cette préoccupation reflète les expériences antérieures en matière d'investissements informatiques traditionnels qui ont donné lieu à des engagements contraignants à long terme. Les services cloud offrent différentes dynamiques en matière de flexibilité des fournisseurs. AWS fournit des services compatibles open source et des options de portabilité des données qui réduisent les obstacles techniques à la migration. Cependant, le compromis entre flexibilité et efficacité opérationnelle reste important. Organisations doivent évaluer la valeur commerciale du maintien des options proposées par les fournisseurs par rapport aux avantages techniques d'une intégration approfondie avec les services spécialisés d'un fournisseur principal.

Certains clients tentent d'éviter d'être bloqués en concevant des solutions indépendantes du cloud qui utilisent des conteneurs. Cette approche les limite souvent aux services de calcul et de stockage de base et contourne les avantages des fonctionnalités avancées du cloud. Notre expérience montre que cette stratégie ajoute une complexité considérable en raison de l'augmentation du temps de développement et des ressources nécessaires, par rapport à l'utilisation de services natifs.

Nos conseils :

- Tenez compte du coût total des architectures indépendantes du cloud. Les frais d'ingénierie supplémentaires ne justifient peut-être pas les avantages liés à la portabilité.
- Utilisez les fonctionnalités natives du cloud pour une valeur maximale. À eux seuls, les services de calcul et de stockage de base sacrifient souvent des avantages significatifs en termes de sécurité, d'évolutivité et d'innovation.
- Planifiez des stratégies cloud en fonction des besoins de l'entreprise. Lorsqu'une implémentation multicloud apporte une valeur ajoutée claire, telle que la capacité de servir les utilisateurs sur plusieurs plateformes, l'investissement technique supplémentaire en vaut la peine.
- Évaluez des scénarios de sortie et des coûts réalistes. Comparez la probabilité et les coûts liés au changement de fournisseur par rapport aux avantages de l'utilisation de l'ensemble complet de Services AWS.
- Tirez parti des bases open source de AWS. AWS les services gérés tels qu'Amazon Relational Database Service (Amazon RDS) vous offrent à la fois flexibilité et excellence opérationnelle, et prennent en charge les moteurs de base de données que vous utilisez aujourd'hui.

- Tirez parti des outils de migration complets fournis par AWS. Nous vous aidons à déplacer les charges de travail dans toutes les directions et nous vous fournissons une sortie de données gratuite si vous partez AWS pour d'autres fournisseurs. Pour plus d'informations, consultez le billet de AWS blog Transfert de données gratuit vers Internet lorsque vous quittez AWS.

Le multicloud améliore la disponibilité et la résilience

La croyance en une commutation fluide des charges de travail entre les fournisseurs de cloud en cas de panne pousse certaines entreprises à adopter des stratégies multicloud. Cet état d'esprit crée une vision simpliste de la résilience de l'infrastructure cloud qui ignore les réalités techniques fondamentales.

Sur la base d'années d'expérience de travail avec des clients multicloud AWS, nous avons constaté que le maintien de la portabilité complète des charges de travail entre les fournisseurs crée souvent une complexité considérable sans apporter tous les avantages escomptés. Les applications gourmandes en données sont confrontées à des défis insurmontables en raison des contraintes de gravité des données. En fait, selon nous, il est quasiment impossible pour les entreprises de mettre en œuvre avec succès un basculement multicloud véritablement fluide pour les charges de travail gourmandes en données.

Lydia Leong, vice-présidente analyste émérite chez Gartner, renforce ce point de vue dans un article publié sur les réseaux sociaux : « Le basculement multicloud est complexe et coûteux au point d'être presque toujours peu pratique, et ce n'est pas un moyen particulièrement efficace de faire face aux risques liés à la résilience du cloud. » La différenciation inhérente entre les fournisseurs en matière de réseau, de stockage, de bases de données, d'apprentissage automatique et de sécurité rend pratiquement impossible une véritable portabilité. La répartition des charges de travail entre les fournisseurs peut augmenter les risques, car une défaillance dans l'un ou l'autre environnement peut provoquer une panne dans tous les environnements.

Nos conseils :

- Concentrez-vous sur la maîtrise AWS des capacités pour les charges de travail individuelles au lieu de vous concentrer sur des architectures multicloud complexes.
- Renforcez la résilience grâce Régions AWS aux zones de disponibilité au lieu de tenter un basculement entre fournisseurs. Pour une analyse technique approfondie de la manière de AWS transférer automatiquement les charges de travail entre les centres de données physiques, consultez le billet de AWS blog intitulé Zonal autoshift — Déplacez automatiquement votre trafic hors des zones de disponibilité lorsque nous détectons des problèmes potentiels.

- Migrez les charges de travail de manière stratégique vers AWS une application à la fois et concentrez-vous sur une application à la fois pour optimiser le succès.

Le multicloud offre de meilleurs prix

La compétitivité des prix est peut-être l'argument le plus faible en faveur des environnements multicloud. L'expérience des entreprises face à des logiciels ou à des contrats de centres de données complexes et coûteux qui les obligent à conclure des contrats pluriannuels les a incitées à se méfier lorsqu'elles achètent des services informatiques. Les approches d'approvisionnement traditionnelles ne se sont pas adaptées aux pay-as-you-go achats, aux remises sur volume ou à la réalité de la concurrence par les prix dans le cloud. (En janvier 2025, AWS a réduit ses prix 151 fois depuis sa création.)

Le principal moteur de réduction des coûts est un environnement cloud bien géré et optimisé. Une entreprise souhaite optimiser ses coûts en travaillant principalement avec un fournisseur dont les services offrent des avantages en termes de rapport qualité-prix (tels que des instances de calcul basées sur des puces conçues sur mesure, telles que AWS Graviton) et qui dispose de solutions de gestion financière dans le cloud de qualité supérieure. Selon une étude menée en 2022 par le Hackett Group auprès de plus de 1 000 entreprises, les dépenses d'infrastructure en pourcentage des dépenses informatiques totales étaient inférieures de 20 % pour les AWS clients par rapport aux entreprises multicloud.

Notre expérience a montré que les entreprises n'anticipent pas les coûts et la complexité supplémentaires liés à l'exploitation de plusieurs clouds, et qu'elles n'évaluent pas correctement ce coût par rapport au gain perçu dans le cadre d'un engagement d' head-to-headapprovisionnement.

Nos conseils :

- Élaborez votre stratégie d'optimisation des coûts sur le pilier d'optimisation des coûts du AWS Well-Architected Framework. Il existe cinq principes de conception :
  - Mettez en œuvre la gestion financière dans le cloud : pour réussir sur le plan financier et accélérer la création de valeur commerciale dans le cloud, vous devez investir dans la gestion financière dans le cloud. Votre organisation doit consacrer le temps et les ressources nécessaires au renforcement des capacités dans ce nouveau domaine de la technologie et de la gestion de l’utilisation. Comme pour vos capacités en matière de sécurité ou d'exploitation, vous devez développer vos capacités par le biais du renforcement des connaissances, des programmes, des ressources et des processus afin de devenir une organisation rentable.

  - Adopter un modèle de consommation : ne payez que les ressources informatiques que vous consommez, et augmentez ou diminuez l'utilisation en fonction des besoins de l'entreprise. Par exemple, les environnements de développement et de test ne sont généralement utilisés que huit heures par jour pendant la semaine de travail. Vous pouvez arrêter ces ressources lorsqu'elles ne sont pas utilisées pour réaliser des économies potentielles de 75 % (40 heures contre 168 heures).
  - Mesurez l'efficacité globale : mesurez le rendement commercial de votre charge de travail et les coûts associés à la livraison. Utilisez ces données pour comprendre les gains que vous réalisez en augmentant la production et les fonctionnalités et en réduisant les coûts.
  - Arrêtez de dépenser de l'argent pour des tâches lourdes et indifférenciées : CSPs effectuez le gros du travail lié aux opérations du centre de données, telles que le montage en rack, l'empilage et l'alimentation des serveurs. Ils suppriment également le fardeau opérationnel lié à la gestion des systèmes d'exploitation et des applications en utilisant des services gérés. Cela vous permet de vous concentrer sur vos clients et vos projets commerciaux plutôt que sur l'infrastructure informatique.
  - Analyser et attribuer les dépenses : le cloud facilite l'identification précise du coût et de l'utilisation des charges de travail, ce qui permet ensuite d'attribuer de manière transparente les coûts informatiques aux flux de revenus et aux différents propriétaires de charges de travail. Cela permet de mesurer le retour sur investissement et offre la possibilité aux propriétaires de charges de travail d'optimiser leurs ressources et de réduire les coûts.
- Compte tenu des frais financiers liés à l'exploitation de différents fournisseurs, nous incitons nos clients à investir massivement dans des outils d'automatisation et d'optimisation des coûts. Chaque CSP propose de nombreux outils natifs dans ce domaine, tels que le Hub d'optimisation des coûts AWS. La plupart des outils natifs offrent d'excellentes fonctionnalités aux clients dans leur environnement cloud. Toutefois, pour comprendre les dépenses entre plusieurs entreprises CSPs, vous pouvez choisir parmi un ensemble complet de produits ISV et de logiciels en tant que service (SaaS) qui étendent ces fonctionnalités afin de fournir une expérience unique permettant d'optimiser les coûts.
- La dilution du pouvoir d'achat par le biais d'une stratégie d'équité des dépenses ne génère pas de valeur commerciale. Cela peut compromettre d'éventuelles remises sur volume et nuire à la conception technique. Le moyen le plus efficace de consommer des services cloud est de faire appel à un fournisseur principal pour la majeure partie de vos opérations et d'en utiliser un autre CSPs uniquement lorsque cela apporte une valeur ajoutée à l'entreprise.

Principe 3. Disposer d'une stratégie et d'une gouvernance claires pour le soutenir

Décider d'adopter une stratégie multicloud ne suffit pas ; vous devez établir une stratégie pour atteindre vos objectifs, notamment une gouvernance claire pour déterminer quelles charges de travail seront transférées où et pourquoi. Les critères d'évaluation doivent être utilisés pour optimiser les charges de travail et leurs dépendances. Si l'évaluation est laissée à l'appréciation des individus, un étalement non coordonné risque d'éroder la valeur de la stratégie multicloud. CSPs Nous vous recommandons d'évaluer régulièrement les performances de la charge de travail du CSP et d'utiliser votre évaluation comme élément clé pour la sélection, les critères et l'utilisation future du CSP.

Une stratégie de gouvernance efficace nécessite une visibilité sur le nombre total de services, d'applications et de composants utilisés dans l'entreprise. Une stratégie de balisage robuste qui couvre CSPs et définit clairement la propriété, l'utilisation et l'environnement (tels que le développement, l'assurance qualité, la mise en scène et la production) pour toutes les ressources déployées font partie intégrante de cette stratégie. Tout doit être associé à un propriétaire ; s'il n'est pas étiqueté ou s'il est impossible d'identifier un propriétaire, il doit être supprimé. Nous travaillons en étroite collaboration avec une grande organisation de services financiers qui trouve et supprime automatiquement toutes les ressources non étiquetées, et considère qu'il s'agit d'une bonne pratique, quels que soient les inconvénients que cela représente pour les équipes de développement. Cette approche de balisage codifie les règles de gouvernance et automatise leur application au lieu de créer des obstacles à la progression (c'est-à-dire qu'elle met en œuvre des barrières de sécurité et non des barrières). Les coûts, les opérations et la sécurité doivent être suivis, surveillés et gérés de la même manière, avec la même profondeur de données et la même transparence CSPs.

Lorsque vous mettez en œuvre une stratégie multicloud, il est essentiel d'établir une structure de compte claire et cohérente pour tous les fournisseurs de cloud afin de maintenir le contrôle opérationnel et la sécurité. Nous vous recommandons d'adopter un hub-and-spoke modèle dans lequel vous créez des éléments distincts Comptes AWS pour les différentes unités commerciales. Ils sont ancrés par deux comptes centraux essentiels : un security/audit compte pour la surveillance consolidée de la conformité et de la sécurité, et un compte réseau central pour la gestion de l'interconnectivité. (Cette approche est codifiée dans la conception de AWS Control Tower. Cependant, les principes du moindre privilège et de la séparation des tâches s'appliquent également aux autres clouds. Le AWS Well-Architected Framework aborde longuement ces concepts et est vivement recommandé aux publics techniques.) Cette approche fondamentale doit être reprise par tous les fournisseurs de cloud afin de maintenir la cohérence de la gouvernance et des opérations.

Les comptes de charge de travail doivent être organisés par environnement (développement, mise en scène, production) ou par fonction, avec des processus clairs établis pour la création et la suppression des comptes.

Nos conseils :

- Mettez en œuvre une stratégie de balisage complète afin de maintenir des modèles de propriété et d'utilisation clairs pour toutes les ressources du cloud. Suivez les environnements, les centres de coûts, les applications et les unités commerciales grâce à des politiques de balisage cohérentes. Supprimez les ressources dépourvues de balises appropriées pour appliquer les normes de gouvernance et préserver la clarté de l'environnement.
- Établissez un cadre de conformité unifié qui cartographie les exigences réglementaires dans votre environnement multicloud. Conservez une documentation claire sur la manière dont les contrôles et les certifications de chaque fournisseur de cloud répondent à vos obligations de conformité.
- Automatisez l'application de la gouvernance grâce à l'automatisation au lieu d'utiliser des processus d'approbation manuels. Codez vos règles de gouvernance dans des systèmes automatisés qui préviennent les violations des politiques avant qu'elles ne se produisent. Cela élimine les erreurs humaines tout en maintenant la vitesse de développement.
- Structurez les comptes dans un hub-and-spoke modèle doté d'une sécurité et d'un contrôle réseau centralisés. Créez des comptes dédiés à l'audit de sécurité et à la gestion du réseau afin de centraliser les fonctions critiques. Cette base permet des politiques de sécurité cohérentes et une connectivité réseau cohérentes au sein de l'entreprise.
- Pour maintenir les limites opérationnelles, créez des comptes, des abonnements ou des projets distincts (selon la nomenclature de votre CSP) pour différents environnements et fonctions. Répartissez les charges de travail par environnements de développement, de préparation et de production. Cette séparation empêche les incidents de sécurité de se propager et permet de maintenir des domaines opérationnels clairs.
- Surveillez les coûts, les opérations et la sécurité grâce à des mesures cohérentes dans l'ensemble de l'environnement. Mettez en œuvre une surveillance unifiée de l'utilisation des ressources, des événements de sécurité et des habitudes de dépenses. Utilisez ces données pour optimiser le placement de la charge de travail et les décisions d'allocation des ressources.
- Empêchez l'utilisation non autorisée du cloud grâce à des politiques organisationnelles et à des contrôles automatisés. Définissez des processus clairs pour la création de comptes et le provisionnement des ressources. Mettez en œuvre des politiques de contrôle des services (SCPs) pour garantir le respect des normes organisationnelles sur tous les comptes.

- Établissez des contrôles de détection et de prévention pour empêcher l'informatique parallèle d'émerger par le biais de comptes de fournisseurs non autorisés. Surveillez l'utilisation non autorisée du cloud grâce aux notes de dépenses et au trafic réseau. Bloquez l'accès non autorisé des fournisseurs tout en préservant les voies d'innovation approuvées.

Principe 4. Ne répartissez pas les charges de travail contiguës entre les clouds

La répartition de charges de travail contiguës entre plusieurs fournisseurs de cloud crée une complexité, des risques et des coûts inutiles. Lorsque les charges de travail qui traitent et analysent les données conjointement concernent plusieurs fournisseurs, les entreprises sont confrontées à des défis en matière de mouvement, de synchronisation et de cohérence des données. Les équipes doivent utiliser des interfaces de gestion APIs, des modèles de sécurité et des processus opérationnels différents pour chaque fournisseur, ce qui augmente le risque d'erreurs et augmente les frais opérationnels. Cette complexité augmente les risques d'erreurs et de surcharge opérationnelle, et peut nuire à l'agilité et à l'évolutivité.

Toutefois, dans certains scénarios pratiques, les entreprises peuvent avoir besoin de répartir des charges de travail contiguës sur les clouds en raison d'exigences commerciales ou techniques spécifiques. Dans ces cas, nous vous recommandons d'établir des critères et des principes directeurs clairs pour évaluer les compromis et de vous assurer que l'approche est conforme à la stratégie multicloud globale de votre organisation.

Lorsque les entreprises choisissent de répartir les charges de travail sur plusieurs clouds, l'adoption d'une architecture centrée sur la messagerie et le couplage souple peut atténuer bon nombre des défis associés. C'est le meilleur moyen de séparer les préoccupations entre les clouds et de réduire l'ampleur de l'impact en cas de défaillance d'un fournisseur. Les opérations les plus limitées dans le temps, telles que les transactions financières, devraient idéalement être conservées dans un environnement unique. Une panne dans un environnement ne doit jamais mettre en danger les charges de travail d'un autre environnement.

Nos conseils :

- Concevez des charges de travail dans le cloud pour garantir l'indépendance opérationnelle afin de minimiser les dépendances en temps réel entre les fournisseurs. Lorsque la répartition de la charge de travail est nécessaire, mettez en œuvre des mécanismes de transfert de données en masse efficaces au lieu de maintenir des connexions intercloud constantes.
- Évaluez chaque charge de travail distribuée proposée par rapport à des critères commerciaux clairs. Tenez compte à la fois des avantages stratégiques et de la complexité opérationnelle induits par la distribution.

Principe 5. Disposer d'une stratégie d'intégration à plus long terme

Soyez prudent lorsque vous déplacez de gros volumes de données entre des applications situées dans différents clouds, en particulier si vos ressources informatiques et vos applications sont déployées dans un CSP et que vos ressources de stockage de données sont déployées dans un autre. Une telle situation peut ajouter de la complexité et du temps de latence susceptibles de neutraliser les avantages perçus. Nous discutons avec de nombreux clients qui disposent d'un lac de données sur un cloud mais qui souhaitent effectuer du machine learning (ML) ou des analyses à l'aide d'outils d'un autre fournisseur de services de traitement des données. Décider où placer les charges de travail dans un environnement multicloud est l'une des décisions les plus cruciales, et souvent les plus difficiles, auxquelles les entreprises sont confrontées. Nous vous recommandons d'évaluer chaque décision de placement de la charge de travail en fonction de trois dimensions critiques : les exigences techniques, les besoins commerciaux et les points forts du fournisseur.

Commencez les évaluations techniques en cartographiant les caractéristiques essentielles de chaque charge de travail : puissance de calcul, opérations de données, besoins en temps de réponse et exigences de croissance. Les applications sont naturellement plus performantes lorsqu'elles sont situées à proximité de leurs données. L'éloignement des applications de leurs sources de données crée des obstacles techniques inutiles et ralentit les performances.

Les décisions commerciales doivent tenir compte de la tarification des fournisseurs, des exigences relatives à la résidence des données et des contrats avec les fournisseurs. Chaque placement de charge de travail a une incidence sur les opérations, la sécurité et la productivité de l'ensemble de l'organisation. L'examen des charges de travail isolément conduit à des décisions sous-optimales.

Nos conseils :

- Mettez en œuvre le transfert de données en masse entre les clouds au lieu d'un accès en temps réel. Planifiez une actualisation périodique des données en utilisant des opérations groupées efficaces au lieu d'utiliser des appels d'API constants entre les clouds. Cette approche permet de réduire les coûts, d'améliorer la fiabilité et de maintenir des performances constantes. Par exemple, exportez des données de ventes quotidiennes résumées au lieu d'interroger des transactions individuelles sur des clouds.
- Tenez compte de la gravité des données lors de la conception du placement de la charge Maintenez les applications à proximité de leurs sources de données principales afin de maintenir

les performances et de réduire les coûts. Les modèles ML, les moteurs d'analyse et les systèmes de traitement des transactions bénéficient tous d'un accès direct à leurs données. Le fait de déplacer ces charges de travail loin de leurs données crée une latence et une complexité inutiles sur le réseau.

- Évaluez les décisions relatives à la charge de travail dans le contexte de votre stratégie cloud complète au lieu de les examiner isolément. Réfléchissez à l'impact de chaque choix de placement sur les processus opérationnels, les contrôles de sécurité et les capacités des équipes au sein de votre organisation. Une décision qui semble optimale pour une seule charge de travail peut compliquer la surveillance ou augmenter les risques de sécurité lorsqu'elle est envisagée de manière globale.
- Définissez des politiques claires de propriété et de gouvernance des données qui spécifient où les différents types de données peuvent résider. Créez un cadre de classification des données qui permet de prendre des décisions cohérentes concernant le placement des données entre les fournisseurs de cloud.

Principe 6. Utiliser les contenants de façon stratégique

Les conteneurs peuvent jouer un rôle important dans le soutien d'une stratégie multicloud, mais il est également important de reconnaître leurs limites. L'utilisation de conteneurs est généralement une bonne idée pour toute application moderne native au cloud, car ils offrent des avantages en termes de portabilité et de cohérence dans différents environnements. Les conteneurs sont indépendants de la plate-forme, ce qui signifie qu'ils peuvent fonctionner sur n'importe quelle plateforme ou infrastructure cloud prenant en charge la technologie de conteneurisation, telle que Kubernetes. Organisations qui utilisent des conteneurs peuvent développer et empaqueter leurs applications une seule fois, puis les déployer de manière cohérente sur plusieurs fournisseurs de cloud ou dans des environnements sur site, sans nécessiter de modifications importantes. En encapsulant le code d'application, les dépendances et l'environnement d'exécution dans un conteneur, vous pouvez atteindre un haut degré de portabilité, ce qui vous permet de déplacer les charges de travail de manière fluide entre les fournisseurs de cloud ou entre le cloud et les centres de données sur site.

Cependant, les conteneurs peuvent ne pas résoudre tous les cas d'utilisation ou éliminer tous les défis auxquels une entreprise peut être confrontée lors de l'adoption d'une stratégie multicloud. Les conteneurs fonctionnent mieux avec les architectures modernes basées sur les microservices, mais ils ne conviennent peut-être pas aussi bien aux grandes applications monolithiques. En outre, bien que les conteneurs puissent traiter certains aspects de la portabilité, tels que l'exécution des applications, ils ne résolvent pas automatiquement les problèmes liés à la gestion des données, aux politiques de sécurité et aux autres dépendances entre les clouds. Organisations doivent encore planifier et concevoir avec soin leurs solutions multicloud afin de garantir une gestion cohérente des données, des contrôles de sécurité unifiés et une intégration parfaite entre les composants hébergés dans le cloud et sur site.

Nos conseils :

- Utilisez les capacités natives de gestion des conteneurs de chaque fournisseur de cloud pour optimiser la valeur commerciale et accélérer la livraison. Cette approche garantit des performances optimales tout en évitant la complexité liée à la création de solutions indépendantes du cloud qui génèrent rarement des rendements significatifs.
- Développez des stratégies de conteneur qui tiennent compte de l'ensemble des opérations, y compris la gestion des données, la sécurité et les dépendances entre les clouds. Concentrez-vous sur les résultats commerciaux lorsque vous prenez des décisions relatives à l'architecture des conteneurs.

Principe 7. Avoir un seul CCo E, mais se spécialiser dans ce domaine

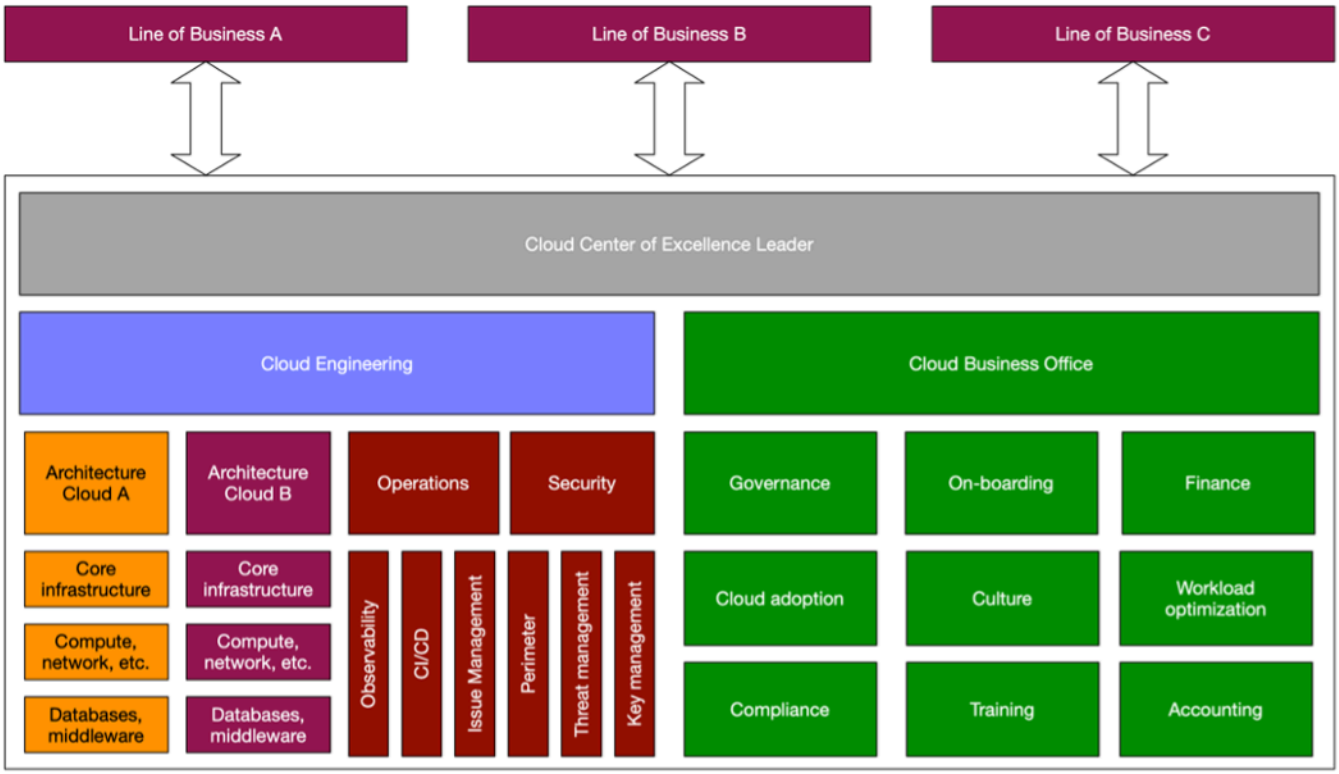
Comme nous le conseillons à de nombreux AWS clients, vous devriez créer un centre d'excellence cloud (CCoE) au sein de votre organisation afin d'assurer le leadership, la standardisation et l'accélération de votre transition vers le cloud. En ce qui concerne les environnements multicloud, nous constatons que les entreprises les plus performantes adoptent une approche équilibrée avec leur E. CCo

Au lieu d'établir CCo des E distincts pour chaque CSP, nous vous recommandons d'avoir un CCo E unique et unifié qui supervise la stratégie multicloud de l'organisation. Cela permet de garantir une approche coordonnée et cohérente plutôt que des efforts cloisonnés susceptibles d'entraîner des divergences, des réingénierie et des gaspillages. Assurez-vous que les équipes de votre CCo E unique disposent des compétences, des outils et des mécanismes spécialisés nécessaires pour chaque CSP utilisé par votre organisation. Ces connaissances spécialisées permettent à l' CCoE de gouverner, de soutenir et d'accélérer l'utilisation des différentes plateformes cloud de manière efficace.

Par exemple, le CCo E devrait avoir AWS des experts spécialisés qui comprennent en profondeur les AWS Cloud services et les meilleures pratiques, ainsi que des experts pour d'autres CSPs personnes capables de guider l'utilisation de ces technologies cloud par l'organisation. Cette expertise spécialisée au sein d'un seul CCo E peut aider votre organisation à bénéficier de la coordination et de la standardisation d'une approche centralisée tout en garantissant que chaque plateforme cloud est utilisée de manière optimale.

Le CCo E unique devrait servir d'organe directeur central chargé d'établir les normes, les politiques et les meilleures pratiques pour la stratégie multicloud de l'organisation. La mise en œuvre effective des charges de travail et des projets cloud peut être confiée à des équipes spécialisées ou à des unités commerciales, tandis que le CCOE assure la supervision, le soutien et la coordination. Cette approche équilibrée permet de garantir une stratégie multicloud cohérente tout en fournissant le degré de flexibilité et d'autonomie nécessaire au sein de l'organisation.

Le schéma suivant montre comment un CCo E peut fournir une approche et une gouvernance centralisées entre plusieurs secteurs d'activité (LOBs), les équipes d'ingénierie cloud et les équipes du Cloud Business Office (CBO).



Nos conseils :

- Structurez votre CCo E pour maintenir une supervision stratégique tout en intégrant une expertise spécialisée pour chaque fournisseur de cloud. Concentrez-vous sur le recrutement d'une expertise approfondie dans le domaine des plateformes cloud individuelles au lieu de rechercher de rares spécialistes du multicloud, et encouragez le partage des connaissances internes pour renforcer les capacités organisationnelles.
- Donnez à votre équipe CCo les moyens d'établir des normes à l'échelle de l'entreprise pour des préoccupations transversales telles que la sécurité et l'observabilité, tout en donnant à chaque équipe l'autonomie nécessaire pour exécuter ces directives en utilisant des outils et des services cloud natifs.
- Développez une stratégie complète en matière de gestion des talents qui concilie une expertise approfondie des principales plateformes cloud avec des connaissances architecturales plus approfondies. Concentrez-vous sur la constitution d'équipes alliant de solides compétences spécifiques au cloud à une expérience en architecture d'entreprise.

Principe 8. Assurez-vous que la sécurité est toujours une priorité absolue

Une approche multicloud complique la tâche en matière de sécurité en augmentant le risque d'accès non autorisé, car votre posture de sécurité doit tenir compte d'un plus grand nombre de surfaces d'attaque. Une stratégie multicloud oblige souvent les entreprises à gérer plusieurs modèles de sécurité CSPs dans des domaines tels que la gestion des identités, la sécurité du réseau, la gestion des actifs et la journalisation des audits. Cette complexité risque de rendre la transparence plus difficile, d'alourdir la charge de travail des équipes de sécurité et d'augmenter les risques.

L'automatisation de la sécurité est essentielle dans les environnements multicloud. La gestion des identités doit fonctionner de manière fluide dans tous les environnements ; elle doit connecter les fournisseurs d'identité existants tout en maintenant des politiques d'accès cohérentes. La sécurité nécessite une protection intégrée des couches des données, du réseau et des terminaux. La classification des données, le chiffrement et la gestion du cycle de vie constituent la base. La sécurité du réseau repose sur des conceptions et des modèles de connexion standardisés. La protection des terminaux complète le cadre grâce à une gestion cohérente des correctifs et à des contrôles basés sur l'hôte.

Ces éléments fondamentaux sont essentiels à l'adoption réussie et sûre de plusieurs fournisseurs de cloud et doivent être pris en compte dès le début de la planification de toute stratégie multicloud.

Nos conseils :

- Mettez en œuvre un cadre de sécurité intégré dans votre environnement multicloud qui se concentre sur trois éléments essentiels : la protection des données grâce à une classification et à un chiffrement normalisés, la sécurité du réseau grâce à des modèles de conception cohérents et la protection des terminaux grâce à des contrôles systématiques et à la gestion des correctifs.
- Établissez un modèle d'opérations de sécurité unifié qui tire parti des capacités de sécurité natives de chaque fournisseur de cloud tout en maintenant une visibilité et un contrôle centralisés grâce à des outils et des processus standardisés.
- Centralisez la collecte et l'analyse des données de sécurité à l'aide d'Amazon Security Lake. Cette plateforme regroupe les informations de sécurité provenant AWS d'autres fournisseurs de cloud, d'applications SaaS et de systèmes sur site dans une vue unique. Il prend en charge l'Open Cybersecurity Schema Framework (OCSF) et permet une analyse standardisée dans

votre environnement hybride et multicloud. Cette approche centralisée améliore la détection des menaces et la réponse aux menaces tout en simplifiant les opérations de sécurité.

- Déployez les outils de sécurité natifs de chaque fournisseur pour améliorer vos capacités de protection. Ces services spécialement conçus répondent aux fonctionnalités spécifiques des fournisseurs tout en renvoyant les données à votre plateforme de sécurité centralisée. La combinaison d'outils natifs et d'une visibilité centralisée permet de fournir une couverture de sécurité complète sur l'ensemble de votre infrastructure.
- Mettez en œuvre une stratégie d'observabilité unifiée qui fournit une visibilité complète sur l'ensemble de votre environnement cloud, y compris les données opérationnelles et de sécurité, à partir de zéro. Optez pour des approches de surveillance de pointe qui permettent un suivi cohérent des services commerciaux, quel que soit l'endroit où ils opèrent.
- Établissez des normes à l'échelle de l'entreprise pour la collecte et la visualisation des données opérationnelles qui permettent d'identifier et de résoudre rapidement les problèmes dans votre environnement multicloud. Concentrez-vous sur la création d'une source unique de vérité pour les informations opérationnelles au service des parties prenantes techniques et commerciales.

Principe 9. Adoptez une approche 80/20 en matière de distribution équitable

La manière dont vous répartissez les charges de travail entre les fournisseurs détermine fondamentalement votre succès dans le multicloud. De nombreuses entreprises recherchent à tort l'égalité dans leur distribution dans le cloud et tentent de répartir les charges de travail de manière égale entre les fournisseurs. Cette approche accroît la complexité sans apporter d'avantages proportionnels. Une distribution équitable fragmente vos capacités techniques, dilue votre pouvoir d'achat et génère des frais opérationnels inutiles. Les équipes ont du mal à développer une expertise approfondie lorsqu'elles sont obligées de maintenir leurs compétences sur plusieurs plateformes simultanément.

L'approche 80/20 fournit des résultats manifestement meilleurs qu'une distribution égale entre les clouds. Le fait de concentrer 80 % de votre investissement auprès d'un fournisseur principal tout en faisant appel à d'autres fournisseurs de manière sélective pour des fonctionnalités spécifiques crée une stratégie équilibrée qui réduit à la fois les coûts et la complexité. Cette approche concentrée accélère l'innovation car vos équipes peuvent développer une expertise approfondie grâce aux services avancés de votre plateforme principale. Votre personnel technique peut devenir spécialiste d'une architecture au lieu de conserver des connaissances superficielles dans plusieurs environnements. Lorsque les ingénieurs maîtrisent une plate-forme, ils créent plus efficacement, résolvent les problèmes plus rapidement et mettent en œuvre des solutions plus sophistiquées.

Les entreprises qui suivent l'approche 80/20 signalent généralement une meilleure rétention des talents, car leurs équipes développent une expertise précieuse et commercialisable au lieu de se contenter de multiples technologies. Cette stratégie concentrée contribue également à simplifier la gestion de la sécurité en limitant la complexité des différents modèles de sécurité des différents fournisseurs. Le cloud principal reçoit la majeure partie de votre investissement dans les outils de sécurité, les solutions de surveillance et les processus opérationnels. Cela crée une base de sécurité plus solide que ce qui est possible avec des ressources réparties de manière égale.

Nos conseils :

- Sélectionnez un fournisseur de cloud principal qui répond à la plupart de vos exigences commerciales et techniques. Ce fournisseur doit prendre en charge au moins 80 % de vos charges de travail et devenir le fondement de votre stratégie cloud. Concentrez vos investissements en formation, vos normes architecturales et vos processus opérationnels sur l'optimisation de la valeur de cette plateforme principale.

- Élaborez des critères clairs pour les charges de travail qui justifient leur placement sur des clouds secondaires. Ces critères doivent se concentrer sur une valeur commerciale spécifique qui ne peut pas être atteinte auprès de votre fournisseur principal. Résistez à placer les charges de travail sur des clouds secondaires simplement pour maintenir l'équité des dépenses ou un équilibre artificiel entre les fournisseurs.
- Structurez vos accords d'entreprise en fonction de votre approche 80/20. Négociez des remises sur volume avec votre fournisseur principal en fonction de la concentration des dépenses, et maintenez la flexibilité avec les fournisseurs secondaires pour des cas d'utilisation spécifiques. Cette approche maximise votre effet de levier d'achat et se traduit généralement par une meilleure tarification globale que la division égale de vos dépenses.
- Alignez votre stratégie de gestion des talents sur votre approche 80/20. Investissez dans le développement d'une expertise approfondie avec les services de votre fournisseur principal tout en conservant une connaissance suffisante des plateformes secondaires pour prendre en charge des charges de travail spécifiques. Cette stratégie ciblée en matière de talents améliore la productivité, accélère les livraisons et réduit le risque de graves pénuries de compétences.
- Mesurez régulièrement les résultats commerciaux de votre stratégie multicloud. Suivez les indicateurs qui démontrent la valeur ajoutée de chaque fournisseur et ajustez votre distribution si nécessaire. L'objectif n'est pas d'éviter complètement le multicloud, mais de le mettre en œuvre de manière stratégique afin que des charges de travail spécifiques bénéficient réellement de fonctionnalités propres aux autres fournisseurs.

Conclusion

Ce paper présente neuf principes clés pour développer une stratégie multicloud efficace. Organisations obtiennent le plus grand succès grâce à une approche du cloud primaire avec l'utilisation stratégique de fournisseurs supplémentaires lorsque des besoins commerciaux spécifiques l'exigent. L'approche 80/20 que nous avons décrite équilibre la concentration et la flexibilité et permet aux entreprises de développer une expertise plus approfondie, de maintenir des relations plus solides avec les fournisseurs et de former des talents plus précieux tout en répondant aux exigences légitimes du multicloud.

Une mise en œuvre réussie du multicloud nécessite une évaluation claire des besoins de l'entreprise au lieu de suivre les tendances du secteur. Les entreprises doivent établir une gouvernance robuste, faire de la sécurité une priorité absolue, éviter de répartir les charges de travail connectées entre les fournisseurs, conserver les applications avec leurs données transactionnelles, reconnaître les limites des conteneurs et maintenir un centre d'excellence cloud unifié mais spécialisé.

L' AWS approche du cloud repose essentiellement sur le choix du client et sur l'interopérabilité. Nous avons conçu nos outils et services pour qu'ils fonctionnent parfaitement dans tous les environnements, car nous savons que les besoins de votre entreprise ne se limitent souvent pas à un seul fournisseur. Des solutions de connectivité hybrides à l'orchestration de conteneurs couvrant plusieurs environnements, elle AWS fournit des fonctionnalités qui vous aident à opérer efficacement dans l'ensemble de votre environnement technologique.

Au lieu de vous obliger à devenir des experts sur de multiples plateformes, elle AWS simplifie la gestion multicloud grâce à des outils intuitifs et à des interfaces cohérentes. Nous nous efforçons d'éliminer la complexité afin que vous puissiez vous concentrer sur l'innovation. Ces fonctionnalités vous aident à mettre en œuvre votre stratégie multicloud selon vos propres conditions, qu'il s'agisse d'utiliser AWS exclusivement ou d'utiliser des environnements spécifiques Services AWS en combinaison avec d'autres environnements.

Le cloud doit renforcer votre stratégie commerciale, et non l'entraver. En appliquant les principes décrits dans ce paper et en tirant parti des fonctionnalités d' AWS interopérabilité, vous pouvez élaborer une approche cloud qui maximise la valeur, minimise la complexité inutile et positionne votre entreprise pour réussir à long terme dans l'environnement commercial dynamique d'aujourd'hui.

Pour en savoir plus sur les AWS solutions qui peuvent aider à simplifier la gestion dans les environnements hybrides et multicloud, consultez la section AWS Solutions pour le multicloud.

Ressources

Références

- Utiliser un centre d'excellence cloud (CCOE) pour transformer l'ensemble de l'entreprise (article de AWS blog)
- AWS Framework Well-Architected
- Identifier les opportunités avec Cost Optimization Hub (AWS Cost Management documentation)
- La valeur commerciale de la migration vers Amazon Web Services (The Hackett Group, février 2022)
- Transfert de données gratuit vers Internet lorsque vous quittez AWS(article deAWS blog)

Outils

- Transfert automatique zonal — Déplacez automatiquement votre trafic hors des zones de disponibilité lorsque nous détectons des problèmes potentiels (AWS article de blog)
- AWS solutions pour le multicloud

AWS Partenaires

- AWS Cloud Compétence opérationnelle

Historique du document

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

Modification	Description	Date
Publication initiale	—	3 septembre 2025

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 :

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

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

A

A2 (1) Agent-to-Agent

Protocole dynamique pour la collaboration agent-agent prenant en charge la délégation de tâches et le transfert d'état.

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

Agent

Un système d'IA capable de raisonner, de planifier et de prendre des mesures de manière autonome à l'aide d'outils pour atteindre des objectifs.

Agent Ops

Pratiques opérationnelles pour la création, le test, le déploiement et l'exécution d'agents d'IA en production à grande échelle.

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 solution 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 Gestion des identités et des accès AWS (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.

blue/green déploiement

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 Mettre en œuvre des procédures permettant de briser le verre dans le AWS Well-Architected guide.

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.

Développeur citoyen

Un utilisateur professionnel qui crée des applications d'intelligence artificielle à l'aide de plateformes sans code/low code sans compétences techniques spécialisées.

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 de stratégie AWS Cloud d'entreprise.

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour 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
- Re-invention — Optimisation des produits et services et innovation dans le cloud

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

CMDB

Consultez la base de données de gestion des configurations.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

défense en profondeur

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 approche de défense approfondie 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 la section Reprise après sinistre des charges de travail sur AWS : Restauration dans le cloud dans le 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 livre, Domain-Driven Design : Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur la manière dont vous pouvez utiliser la conception axée sur le domaine avec le modèle Strangler Fig, consultez la section Modernisation incrémentielle des anciens services Web ASP.NET Microsoft (ASMX) à l'aide de conteneurs et d'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.

EDI

Voir échange de données informatisé.

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

Ordre dans lequel les octets sont stockés dans la mémoire de l'ordinateur. Big-endian les systèmes stockent d'abord l'octet le plus significatif. Little-endian les systèmes 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 principaux Comptes AWS ou à Gestion des identités et des accès AWS (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.

- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un CI/CD pipeline, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

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.

invitation en quelques coups

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

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le modèle de fondation.

modèle de fondation (FM)

Un vaste réseau neuronal d'apprentissage profond qui s'entraîne sur des ensembles de données massifs de données généralisées et non étiquetées. Les FM sont capables d'effectuer une grande variété de tâches générales, telles que la compréhension du langage, la génération de texte et d'images et la conversation en langage naturel. Pour plus d'informations, voir Que sont les modèles de base ?

Passerelle FM

Un intermédiaire centralisé qui contrôle et normalise l'accès aux modèles de base. Également connue sous le nom de passerelle LLM.

G

IA générative

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

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

Sur Amazon CloudFront, option permettant d'empêcher les utilisateurs de certains pays d'accéder aux distributions de contenu. Vous pouvez utiliser une liste d'autorisation ou une liste de blocage

pour spécifier les pays approuvés et interdits. Pour plus d'informations, consultez la section Restreindre la distribution géographique de votre contenu dans la CloudFront documentation.

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités 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 CSPM GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

rambardes (AI)

Des mécanismes de sécurité qui filtrent, valident et limitent les entrées et sorties des agents afin de garantir un comportement responsable et sûr de l'IA.

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation des historiens

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

données de rétention

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

humain dans la boucle (HiTL)

Un modèle de flux de travail dans lequel l'exécution des agents s'arrête pour examen et approbation par l'homme aux points de décision critiques.

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. AI/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, voir Interprétabilité du modèle d'apprentissage automatique avec AWS.

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

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

grand modèle de langage (LLM)

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

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

lift and shift

Voir 7 Rs.

système de poids faible

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

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

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

branche principale

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

MCP

Voir Model Context Protocol.

Protocole de contexte du modèle (MCP)

Protocole sans état pour la communication entre un agent et un outil.

serveur MCP

Service qui expose un ou plusieurs outils via le protocole Model Context.

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 AWS Well-Architected cadre.

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)

Un protocole de communication léger de machine à machine (M2M), basé sur le publish/subscribemodèle, 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

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

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration. Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les

exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le AWS compte.

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

Protocole de communication machine à machine (M2M) pour l'automatisation industrielle. OPC-UA fournit une norme d'interopérabilité avec des schémas de chiffrement, 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 Examens de l'état de préparation opérationnelle (ORR) dans le AWS Well-Architected cadre.

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). OAC prend en charge tous les compartiments S3 dans leur ensemble Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les `DELETE` requêtes dynamiques `PUT` adressées au compartiment S3.

identité d'accès d'origine (OAI)

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

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS multi-comptes, un VPC qui gère les connexions réseau initiées depuis une application. L'architecture 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.

policy

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.

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

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.

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

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

Q

plan de requête

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

régression du plan de requêtes

Le cas où un optimiseur de service de base de données choisit un plan moins optimal qu'avant une modification donnée de l'environnement de base de données. Cela peut être dû à des

changements en termes de statistiques, de contraintes, de paramètres d'environnement, de liaisons de paramètres de requêtes et de mises à jour du moteur de base de données.

R

Matrice RACI

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

RAG

Voir Retrieval Augmented Generation.

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Région

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.

Génération augmentée de récupération (RAG)

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

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de temps de rétablissement.

runbook

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

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs qui vous aident à mettre en œuvre les meilleures pratiques en matière 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.

IA de l'ombre

Applications d'IA non autorisées créées ou utilisées en dehors des canaux régis au sein d'une organisation.

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.

modèle split-and-seed

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 un exemple d'application de ce modèle, consultez la section Modernisation progressive des anciens services Web Microsoft ASP.NET (ASMX) à l'aide de conteneurs et d'Amazon API Gateway.

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

tags

Key-value des paires 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.

outil

Fonction ou API qu'un agent peut invoquer pour effectuer des opérations dans des systèmes externes.

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.

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

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

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité 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.

invite Zero-Shot

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

application zombie

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

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