Investir dans l'ingénierie du chaos en tant que nécessité stratégique

AWS Directives prescriptives

AWS Directives prescriptives: Investir dans l'ingénierie du chaos en tant que nécessité stratégique

Table of Contents

Investir dans l'ingénierie du chaos en tant que nécessité stratégique

Adrian Hornsby, Amazon Web Services

Janvier 2025 (historique du document)

Les pratiques d'ingénierie du chaos utilisent des perturbations contrôlées pour identifier les problèmes du système et les opportunités afin de prévenir les pannes et autres incidents. L'ingénierie du chaos est devenue essentielle pour améliorer la résilience des systèmes, mais son adoption généralisée se heurte à des obstacles liés aux idées fausses, à la résistance culturelle, aux ressources et à la quantification de la valeur commerciale. La définition d'objectifs initiaux permet de relancer les efforts d'ingénierie du chaos, tandis que la quantification du retour sur investissement (ROI) justifie la poursuite des investissements, en particulier dans un contexte de pressions économiques.

Ce document de stratégie décrit une approche holistique visant à saisir à la fois les améliorations opérationnelles quantitatives et les avantages organisationnels qualitatifs. L'objectif ultime est de traiter l'ingénierie du chaos comme une nécessité stratégique au même titre que la cybersécurité et non comme un exercice continu de justification des coûts.

Coûts des temps d'arrêt et émergence de l'ingénierie du chaos

L'Information Technology Intelligence Consulting (ITIC) estime que 90 % des entreprises sont confrontées à des coûts supérieurs à 300 000 dollars par heure d'indisponibilité, et 41 % supérieurs à 1 à 5 millions de dollars par heure. Outre les pertes de revenus immédiates, les temps d'arrêt peuvent entraîner des problèmes à long terme, notamment des manquements à la conformité, une baisse du cours des actions, des coûts d'atténuation importants et même une atteinte à la marque.

Bien que les temps d'arrêt soient généralement associés aux systèmes en ligne générateurs de revenus, l'impact négatif va bien au-delà de cela. Toutes les grandes entreprises et organisations, quel que soit leur principal modèle de revenus, dépendent de manière essentielle de la disponibilité de leurs systèmes internes, tels que les ressources humaines et la paie.

Les interruptions de service affectant ces services internes essentiels peuvent entraver la capacité d'une entreprise à fonctionner, entraînant des perturbations opérationnelles importantes et des répercussions financières. Les problèmes qui en résultent peuvent inclure les suivants :

- Retards dans le paiement des employés et des fournisseurs
- Incapacité de traiter les commandes ou les transactions des clients
- Violations de données sensibles autorisées par des systèmes de sécurité compromis
- Perte de productivité et opportunités de revenus
- Sanctions réglementaires en cas de non-conformité
- Atteinte à la réputation de la marque

L'ingénierie du chaos introduit intentionnellement des perturbations contrôlées. L'utilisation de l'ingénierie du chaos pour comprendre ou vérifier la réponse du système aux défaillances est devenue une pratique essentielle pour améliorer la résilience du système. L'ingénierie du chaos permet à votre organisation de détecter les problèmes de manière proactive, de valider les mécanismes de résilience et, en fin de compte, de réduire le risque d'interruptions imprévues et les coûts associés. Les avantages de l'ingénierie du chaos sont les suivants :

- Exposer la dette technique
- Exercer les muscles opérationnels

- Renforcer la confiance dans les systèmes
- Identifier les points de défaillance
- Améliorer le suivi et l'observabilité
- Soutenir l'apprentissage basé sur l'expérience
- Améliorer la résilience pour réduire les temps d'arrêt

À mesure que les systèmes deviennent plus complexes et que les attentes des clients augmentent, l'ingénierie du chaos prend de plus en plus d'importance. Gartner recommande l'ingénierie du chaos comme pratique essentielle pour les entreprises afin de réduire les temps d'arrêt imprévus et d'améliorer la résilience.

Les défis de l'adoption de l'ingénierie du chaos

Bien que l'ingénierie du chaos soit une pratique de plus en plus importante pour améliorer la résilience des systèmes, son adoption peut se heurter aux obstacles suivants :

- Perceptions erronées à propos du risque – Une idée fausse courante est que l'ingénierie du chaos n'est menée que dans les environnements de production, ce qui suscite des inquiétudes quant aux risques excessifs. Cette perception provient d'un manque de compréhension de la nature systématique et contrôlée des pratiques d'ingénierie du chaos. Comme indiqué dans le AWS Well-Architected Framework, effectuez d'abord une simulation de panne dans un environnement hors production.
- Valeur commerciale à plus long terme – Les avantages de Chaos Engineering augmentent progressivement, ce qui rend difficile la quantification de la valeur commerciale et la justification de l'investissement initial. En raison du retour sur investissement plus lent, les entreprises ont du mal à établir des priorités et à s'en tenir à l'ingénierie du chaos.
- Lacunes en matière de compétences et d'expertise – L'ingénierie du chaos nécessite un ensemble unique de compétences et d'expertise qui ne sont peut-être pas facilement disponibles au sein de votre organisation. Le développement ou l'acquisition de cette expertise peuvent constituer un obstacle important, en particulier pour les organisations qui débutent dans cette pratique et celles dont les ressources sont limitées.

Le reste de ce document de stratégie se concentrera principalement sur le deuxième défi, qui consiste à démontrer la valeur commerciale de l'ingénierie du chaos.

Les effets cumulatifs de l'ingénierie du chaos

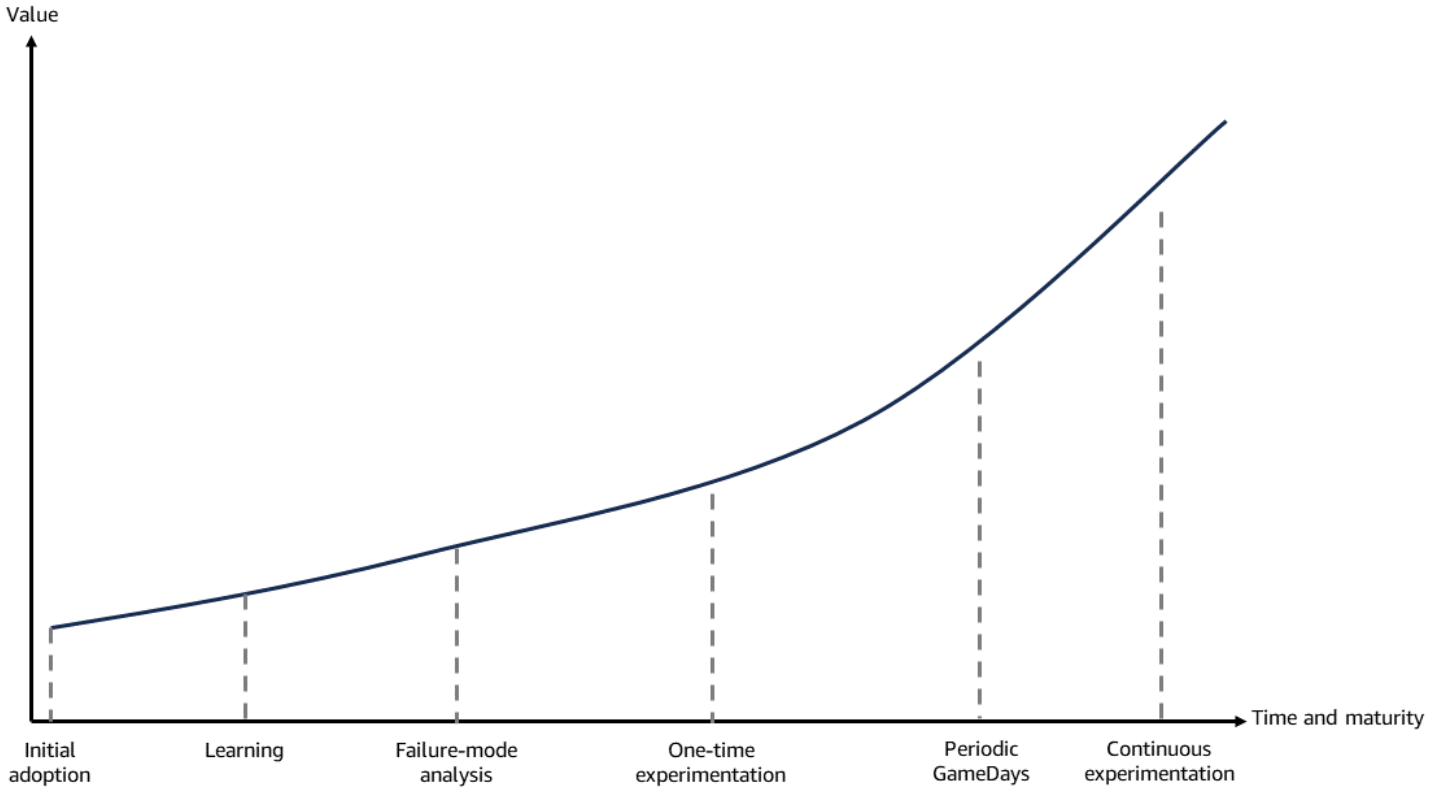
Contrairement aux projets technologiques traditionnels dont les dates de début et de fin sont bien définies, l'ingénierie du chaos est une pratique continue d'apprentissage continu et d'amélioration continue de la résilience du système. Les avantages de l'ingénierie du chaos se multiplient au fil du temps.

À mesure que les systèmes évoluent et se complexifient, de nouveaux modes de défaillance apparaissent. D'autres expériences sur le chaos sont nécessaires pour identifier les problèmes potentiels. La résolution d'un problème peut prendre des mois, en particulier dans les grandes entreprises dotées de systèmes et de processus complexes, ou lorsque les défaillances sont le fait de fournisseurs de services externes.

Le changement culturel qui consiste à considérer l'échec comme une opportunité d'apprentissage et d'amélioration prend de l'ampleur au fil des années et s'ancre dans l'organisation. Les investissements dans l'automatisation des expériences d'ingénierie du chaos et le développement d'outils de soutien continuent de rationaliser et d'améliorer les pratiques d'ingénierie du chaos. L'acquisition de ces connaissances institutionnelles et de cette compréhension de la résilience du système est un processus graduel qui s'accumule au fil du temps. Les connaissances, les processus et les outils développés grâce à l'ingénierie du chaos gagnent en valeur à mesure que la pratique évolue parallèlement à l'évolution constante des systèmes.

Le schéma suivant montre comment la valeur augmente au fil du temps à mesure que l'adoption du chaos progresse selon les étapes suivantes :

- Adoption initiale
- L'apprentissage
- Analyse du mode défaillance
- Expériences ponctuelles
- Périodique GameDays
- Expérimentation continue



Comme le montre le schéma, les avantages de l'ingénierie du chaos commencent souvent avant qu'un défaut ne soit injecté dans le système. Le processus de planification et de conception d'expériences de chaos lui-même apporte une valeur immédiate. L'identification des scénarios de défaillance potentiels, des points de défaillance uniques et des zones d'incertitude dans le système permet d'apporter des améliorations.

Par exemple, la rédaction de scénarios de défaillance et la discussion des effets en cascade potentiels, un processus appelé analyse des modes de défaillance et des effets (FMEA) permet de découvrir des faiblesses ou des lacunes évidentes qui auraient pu être négligées. Votre organisation peut résoudre ces problèmes de manière proactive, avant même de soumettre le système à des perturbations intentionnelles. Pour plus d'informations, consultez le cadre d'analyse de résilience.

En outre, l'attention accrue portée à l'observabilité et à la surveillance du système qui accompagne souvent les initiatives d'ingénierie du chaos commence à porter ses fruits immédiatement. L'amélioration de la visibilité du comportement du système et des modes de défaillance aide l'équipe à mieux comprendre les conditions de fonctionnement normales du système. Une meilleure visibilité permet également à l'équipe de comprendre comment les conditions de fonctionnement se dégradent, s'adaptent et échouent lorsqu'elles sont poussées à leurs limites.

Les GameDay modes d'expérience ponctuelle et périodique sont des approches plus manuelles que le mode d'expérimentation continue. Ils nécessitent un processus plus pratique et exploratoire, dans le cadre duquel les ingénieurs élaborent et affinent activement les hypothèses par le biais de leurs observations et expériences.

Le mode d'expérimentation continue est, en revanche, de nature plus automatisée. Ce mode se concentre sur l'exécution d'hypothèses approuvées et validées de manière contrôlée et itérative. Il utilise l'automatisation et l'intégration dans le processus de développement par le biais d'un pipeline de chaos dédié pour garantir des expériences cohérentes et reproductibles.

Initiatives locales d'ingénierie du chaos

Le parcours d'ingénierie du chaos commence souvent au niveau local, où les équipes d'ingénierie identifient les besoins et commencent à expérimenter l'ingénierie du chaos de manière indépendante.

Dans le cadre de cette approche locale, les équipes expérimentent, apprennent et affinent leurs pratiques d'ingénierie du chaos. La valeur de l'ingénierie du chaos peut être démontrée par les résultats tangibles suivants :

- Réduction du nombre d'incidents
- Meilleure observabilité
- Temps de restauration plus rapides
- Résilience améliorée et continue du système

Les initiatives locales d'ingénierie du chaos émergent généralement dans des conditions organisationnelles spécifiques. Ils ont besoin d'un environnement doté d'un haut degré d'autonomie technique, dans lequel les équipes ont la liberté d'expérimenter et d'innover sans obstacles bureaucratiques excessifs. L'expertise locale en ingénierie de résilience ou en systèmes distribués est cruciale, car elle fournit les bases techniques nécessaires à la compréhension et à la mise en œuvre d'expériences de chaos. Plus important encore, ces initiatives s'appuient souvent sur des champions du chaos, des personnes passionnées qui comprennent la valeur de l'ingénierie du chaos. Les champions du chaos sont prêts à plaider en faveur de l'adoption de l'ingénierie du chaos, à former leurs pairs et à mener les premières expériences. Sans liberté organisationnelle, sans expertise technique et sans champions motivés, les efforts locaux d'ingénierie du chaos prennent rarement racine, quels que soient leurs avantages potentiels.

Le rôle des objectifs dans l'adoption de l'ingénierie du chaos

Il est courant que les objectifs initiaux émergent de manière organique des efforts d'ingénierie du chaos déployés au sein d'une organisation. Poussés par le besoin de résoudre leurs propres problèmes récurrents, ces équipes ou groupes explorent souvent les pratiques d'ingénierie du chaos sans approbation explicite ni hiérarchisation des niveaux supérieurs.

Les équipes peuvent utiliser ces résultats pour présenter des arguments convaincants en faveur d'une adoption organisationnelle plus large, devenant ainsi un terrain d'essai pour les autres équipes.

Lorsque les avantages des efforts locaux deviennent trop importants pour être ignorés, ces équipes peuvent élever leurs efforts et leurs connaissances au niveau du leadership et se fixer des objectifs. Cette visibilité accrue peut faciliter l'adoption d'objectifs de résilience à l'échelle de l'organisation et fournir le soutien et les ressources nécessaires à la mise en œuvre de l'ingénierie du chaos.

Les objectifs, en particulier ceux définis par le leadership et établis en réponse à des pannes importantes, jouent un rôle crucial dans l'adoption de pratiques d'ingénierie du chaos. Les types d'objectifs les plus courants sont les suivants :

- Objectifs de disponibilité pour identifier et réduire les points de défaillance uniques (SPOF)
- Objectifs de reprise des services pour améliorer la capacité de reprise après une interruption ou une panne
- Objectifs en matière d'expérience utilisateur pour atteindre des objectifs de niveau de service spécifiques () SLOs
- Objectifs basés sur des indicateurs pour suivre les progrès réalisés en matière d'atténuation des risques de disponibilité connus et de mise en œuvre des mesures de résilience recommandées
- Objectifs réglementaires et de conformité pour démontrer la résilience opérationnelle

Pour plus d'informations sur certains de ces types d'objectifs et sur la manière dont Amazon et d'autres organisations ont utilisé les objectifs lors de l'adoption de l'ingénierie du chaos, consultez l'annexe A.

Ces objectifs constituent une justification convaincante et fournissent une approche ciblée et réalisable pour favoriser l'adoption de l'ingénierie du chaos. Au début, les objectifs servent d'indicateur pour les indicateurs de retour sur investissement traditionnels. Les objectifs fournissent une justification convaincante lorsqu'il peut être difficile d'obtenir des calculs quantifiables de retour

sur investissement en matière de résilience. Sans de tels objectifs dès le début de l'adoption, la pratique de l'ingénierie du chaos risque de ne pas démontrer son efficacité et de gagner une plus grande adhésion organisationnelle.

Passer des objectifs à la mesure du retour sur investissement

Au fur et à mesure que les pratiques évoluent et que les objectifs initiaux sont atteints, l'accent est finalement mis sur la quantification des avantages financiers tangibles de l'ingénierie du chaos, à savoir le retour sur investissement (ROI). Ce changement s'explique principalement par deux raisons :

- Considérations économiques
- Préserver l'expérience client et la confiance

Considérations économiques

En période de croissance économique et de finances saines, les entreprises n'ont souvent pas besoin de justifications détaillées pour fixer des objectifs spécifiques en matière de stratégies d'ingénierie du chaos. Cependant, l'évolution du paysage financier a amené de nombreuses entreprises à réévaluer leurs investissements, et les mises en œuvre de l'ingénierie du chaos doivent fournir un retour sur investissement quantifié.

Ces entreprises sont désormais chargées de définir des indicateurs de retour sur investissement clairs et traditionnels afin de démontrer la valeur et l'impact des pratiques d'ingénierie du chaos. Ce défi est encore compliqué par le paradoxe de la prévention. Le paradoxe de la prévention se produit lorsqu'une prévention efficace des incidents rend plus difficile la justification de l'investissement, car les parties prenantes ont tendance à sous-évaluer les catastrophes évitées. Même les organisations dotées d'une culture d'excellence opérationnelle profondément ancrée sont obligées d'utiliser des indicateurs de retour sur investissement pour justifier l'adoption continue de l'ingénierie du chaos.

Préserver l'expérience client et la confiance

Le maintien d'une résilience axée sur les objectifs peut s'avérer difficile à long terme. Une fois qu'un objectif initial, tel que l'atteinte d'un objectif de temps de reprise, est atteint, il devient difficile de justifier un investissement continu dans l'ingénierie du chaos jusqu'à la prochaine panne majeure. Le flux et le reflux des investissements créent un cycle en dents de scie réactif. À chaque nouvelle panne, l'investissement dans la résilience augmente avec un nouvel objectif qui s'attaque à la cause

première. Une fois le nouvel objectif atteint, l'investissement diminue jusqu'au prochain incident, relançant ainsi la boucle réactive.

Les pannes qui sous-tendent cette approche réactive ont un impact négatif sur les clients. La question clé : combien de pannes majeures les clients toléreront-ils avant d'abandonner un fournisseur de services au profit d'un concurrent plus résilient ?

Quantifier le retour sur investissement de l'ingénierie du chaos

À l'heure actuelle, très peu de ressources publiées fournissent des méthodologies complètes ou des données réelles pour quantifier le retour sur investissement (ROI) à long terme de l'ingénierie du chaos.

Dans le paper The Business Case for Chaos Engineering, Netflix propose une équation précieuse pour calculer le retour sur investissement de l'ingénierie du chaos. Cette équation constitue un point de départ pour les entreprises qui se lancent dans l'ingénierie du chaos.

L'équation exige que vous estimiez avec précision les coûts des éléments suivants :

- Pannes évitables et non évitables
- Coûts de mise en œuvre d'un programme d'ingénierie
- Coûts des dommages induits par le chaos

Les dommages provoqués par le chaos font référence à l'impact négatif ou à la perturbation causés par l'injection délibérée de défaillances ou de conditions turbulentes dans un système dans le cadre d'expériences d'ingénierie du chaos. L'équation nécessite d'estimer les coûts des pannes évitables et non évitables, les coûts de mise en œuvre des programmes d'ingénierie du chaos et les coûts des dommages induits par le chaos.

Il est difficile de déterminer avec certitude quels problèmes auraient pu être évités grâce à un programme d'ingénierie du chaos. Cela nécessite une analyse hypothétique qui consiste à examiner les causes profondes des problèmes et à spéculer sur la manière dont les expériences d'ingénierie du chaos auraient pu aider à les identifier. Cette analyse est difficile car les systèmes modernes sont très complexes, avec de nombreuses interdépendances et interactions entre différents composants, services et bibliothèques tierces. De plus, les défaillances des systèmes sont souvent non déterministes, et les conditions à l'origine des défaillances peuvent être difficiles à comprendre avec le recul.

Bien que l'approche suggérée par Netflix présente certaines limites, elle constitue une bonne base pour les organisations qui commencent à explorer l'ingénierie du chaos. L'équation peut vous aider à estimer les coûts et les avantages potentiels, ce qui vous aide à prendre des décisions concernant la mise en œuvre d'un tel programme. Cependant, au fur et à mesure que les entreprises

progressent dans leur parcours d'ingénierie du chaos, il est important d'étendre l'évaluation du retour sur investissement afin d'intégrer une perspective plus globale.

Cette approche holistique permettra non seulement de tirer parti des avantages directs de la réduction des pannes et des coûts d'ingénierie, mais également de mettre en évidence les effets transformateurs à long terme sur la résilience globale de l'organisation. Il capture les avantages cumulatifs et les effets organisationnels plus larges de l'ingénierie du chaos afin de donner une représentation plus précise de la valeur et de l'impact réels de l'ingénierie du chaos.

Une approche globale de la quantification du retour sur investissement

Une évaluation globale du retour sur investissement doit prendre en compte non seulement des mesures quantitatives, mais également des facteurs qualitatifs. L'approche holistique nécessite des données réelles provenant d'organisations qui pratiquent l'ingénierie du chaos à grande échelle sur de longues périodes. Vous pouvez utiliser des données provenant de projets et d'objectifs locaux par le biais de toutes les données de retour sur investissement que vous avez collectées selon une approche par équation.

Les mesures quantitatives se concentrent sur les quantités ou les fréquences. Les mesures sont objectives et peuvent être analysées statistiquement. Les exemples incluent des enquêtes, des expériences et des analyses de données. Les mesures quantitatives peuvent inclure les suivantes :

- Métriques relatives aux incidents
- Coûts
- Améliorations
- Conformité d'
- Taux d'adoption
- Satisfaction du client

Le suivi des mesures quantitatives peut démontrer les avantages opérationnels directs de l'ingénierie du chaos.

Les mesures qualitatives sont descriptives et visent à comprendre les expériences et les opinions. Ils sont souvent subjectifs et ne peuvent pas être facilement mesurés numériquement. Pour l'ingénierie

du chaos, les mesures qualitatives capturent les impacts organisationnels plus larges. Les mesures qualitatives peuvent inclure les suivantes :

- Confiance des employés
- Changement culturel
- Collaboration
- Efficacité de la formation
- Rétention des talents
- Réputation de la marque
- Avantage compétitif

En tenant compte à la fois des impacts financiers quantitatifs et des avantages organisationnels qualitatifs, vous pouvez prendre des décisions plus éclairées concernant la poursuite des investissements dans l'ingénierie du chaos tout en favorisant une culture de résilience.

Pour plus d'informations sur ces mesures et le cadre de classification des incidents qui leur est associé, voir les annexes B et C.

Passer du retour sur investissement à l'ingénierie du chaos en tant que nécessité stratégique

Bien qu'il soit tentant de surveiller le retour sur investissement, les défis liés à la mesure de la valeur de l'ingénierie du chaos amènent souvent les entreprises à privilégier les gains d'efficacité immédiats et à court terme par rapport aux investissements stratégiques dans la résilience. Cette approche ne tient pas compte de l'ingénierie du chaos en tant que moteur clé de la résilience et des avantages concurrentiels liés à la prévention des pannes. La véritable valeur de l'ingénierie du chaos réside dans la prévention de futures défaillances. L'ingénierie du chaos soutient la continuité des activités à long terme.

Au lieu de vous concentrer sur le retour sur investissement, considérez l'ingénierie du chaos comme la cybersécurité. Comme expliqué dans l'article de Forbes La cybersécurité en tant qu'investissement stratégique : comment l'optimisation du retour sur investissement peut mener à un avenir plus sûr, la cybersécurité ne doit pas être considérée comme un centre de coûts ou une dépense obligatoire pour les entreprises, car cet état d'esprit ne tient pas compte de la valeur stratégique que des mesures de cybersécurité robustes peuvent apporter au fil du temps. L'auteur soutient plutôt qu'en modifiant les perspectives pour considérer la cybersécurité comme un investissement à long terme générateur d'avantages concurrentiels, les entreprises peuvent ouvrir de nouvelles voies d'innovation, d'efficacité opérationnelle et de différenciation sur leurs marchés respectifs. En adoptant cette approche, l'auteur conclut que les responsables de la sécurité de l'information (CISOs) peuvent mieux obtenir l'adhésion et le financement des dirigeants. Ils peuvent ensuite positionner leurs entreprises de manière à devancer leurs concurrents dans un environnement cybernétique de plus en plus risqué. Cette création de valeur stratégique à long terme de la cybersécurité est parallèle aux améliorations continues inhérentes aux pratiques d'ingénierie du chaos.

Alors que la sécurité protège la capacité d'une entreprise à exploiter et à protéger ses actifs, l'ingénierie du chaos contribue à garantir la disponibilité, la fiabilité et la capacité de restauration des principaux systèmes et services. Pour obtenir une valeur à long terme et un avantage concurrentiel, considérez l'ingénierie du chaos comme une capacité essentielle et un impératif stratégique, et non comme une initiative nécessitant une justification constante.

Le schéma suivant montre l'évolution de l'ingénierie du chaos, de la base aux objectifs et au retour sur investissement, pour devenir une stratégie.

Au niveau local, les équipes expérimentent généralement de manière indépendante, en fonction des besoins locaux. Ces expériences sont soutenues par des ingénieurs passionnés qui démontrent leur valeur en réduisant le nombre d'incidents et en améliorant l'observabilité.

Lorsque ces efforts sont couronnés de succès, les équipes peuvent élever leur apprentissage au niveau du leadership. Grâce à cette visibilité, les efforts passent à une phase axée sur les objectifs. L'organisation définit des objectifs formels en matière de résilience et de reprise, soutenus par des ressources et un soutien pour une mise en œuvre plus large.

Enfin, l'ingénierie du chaos atteint la maturité au-delà de l'exigence constante de justification du retour sur investissement pour être reconnue comme une nécessité stratégique, au même titre que la cybersécurité. À ce stade, l'ingénierie du chaos est totalement intégrée aux processus organisationnels. La mise en œuvre se concentre sur la résilience à long terme plutôt que sur des indicateurs à court terme. L'ingénierie du chaos est considérée comme une capacité essentielle au maintien de l'avantage concurrentiel et de la confiance des clients.

Intégrer l'ingénierie du chaos dans votre organisation

Pour donner à l'ingénierie du chaos la même importance qu'à la sécurité, tenez compte des suggestions suivantes :

- Faire de l'ingénierie du chaos une pratique non négociable – Tout comme la cybersécurité est considérée comme une exigence fondamentale pour les organisations, considérez l'ingénierie du chaos comme une pratique obligatoire pour garantir la résilience et la fiabilité du système. Intégrez l'ingénierie du chaos dans les processus, les outils et la culture de votre organisation, plutôt que de la considérer comme une activité facultative ou discrétionnaire. Pour plus d'informations, consultez le guide Resilience Lifecycle Framework.
- Garantir l'adhésion et le soutien de la direction – Comme pour les initiatives de sécurité, les efforts d'ingénierie du chaos doivent bénéficier de l'adhésion et du soutien actif de la direction. Cela inclut l'allocation de ressources, de budgets et de personnel dédiés à la mise en œuvre et au maintien des pratiques d'ingénierie du chaos au sein de l'organisation.

- Mettre en œuvre la gouvernance et la supervision – À l'instar d'un CISO et d'un cadre de gouvernance de la sécurité, mettez en place une équipe dédiée à l'ingénierie du chaos ou un responsable de la résilience. Cette équipe ou ce rôle est chargé de superviser et de coordonner les efforts d'ingénierie du chaos au sein des différentes équipes et unités commerciales.
- Intégrez l'ingénierie du chaos dans les cycles de développement et d'exploitation – Tout comme les pratiques de sécurité sont intégrées aux processus de développement et de déploiement des logiciels, faites de l'ingénierie du chaos une partie intégrante du cycle de développement et de livraison des logiciels.
- Menez régulièrement des exercices et des simulations d'ingénierie du chaos – À l'instar des simulations de failles de sécurité et des exercices de réponse aux incidents, menez régulièrement des expériences d'ingénierie du chaos pour valider les capacités de réponse aux incidents et identifier les angles morts potentiels de manière proactive.
- Utilisez l'ingénierie du chaos pour gérer les runbooks – Comme pour les examens de sécurité, utilisez des expériences d'ingénierie du chaos pour valider l'efficacité et la précision des runbooks en matière de réponse aux incidents et de restauration. En outre, les expériences d'ingénierie du chaos peuvent servir de simulations réalistes permettant aux ingénieurs de garde de s'entraîner à exécuter les procédures du runbook. Les simulations aident les ingénieurs à conserver leur mémoire musculaire opérationnelle et à se préparer à faire face à des incidents réels.
- Favoriser une culture de résilience – Comme pour les formations de sensibilisation à la sécurité, investissez dans la formation en ingénierie du chaos et dans des initiatives de partage des connaissances afin de favoriser une culture de résilience. Incluez des programmes de formation, une collaboration interfonctionnelle et des incitations pour les équipes qui adoptent des pratiques d'ingénierie du chaos.
- Mesurez les indicateurs de résilience et établissez des rapports sur ceux-ci – Surveillez régulièrement les indicateurs de résilience et signalez-les aux parties prenantes. Utilisez les indicateurs quantitatifs et qualitatifs présentés dans ce document comme point de départ.
- Considérez la résilience comme un avantage concurrentiel – Les mesures de cybersécurité peuvent fournir un avantage concurrentiel. De même, considérez vos capacités d'ingénierie du chaos et de résilience comme un facteur de différenciation qui vous permet d'offrir des services plus fiables et dignes de confiance à vos clients.

Obtenir l'adhésion de la direction

L'ingénierie du chaos n'a souvent pas de propriétaire clair parmi les responsabilités traditionnelles de la haute direction. Le PDG se soucie de la croissance, de la rentabilité et du leadership sur le

marché. Le directeur financier se concentre sur la performance financière, le contrôle des coûts et la gestion des risques. Le CTO donne la priorité à la stratégie technologique, aux feuilles de route des produits et à l'excellence en ingénierie. Le CISO supervise la sécurité et la conformité.

Comme aucun dirigeant ne possède véritablement la résilience, il est souvent difficile d'obtenir l'adhésion et le soutien nécessaires. Pourtant, les défaillances du système ont un impact sur les revenus, la satisfaction des clients et la réputation de la marque, ce qui préoccupe le PDG et le directeur financier. Le CTO et le CISO sont chargés de mettre en œuvre des mesures de résilience, mais ils peuvent ne pas avoir de mandat organisationnel. Cette ambiguïté peut empêcher de réaliser des investissements stratégiques et d'aligner l'organisation sur une stratégie de résilience commune.

Cette ambiguïté complique également l'obtention de l'adhésion des dirigeants à des initiatives de résilience telles que l'ingénierie du chaos. Après tout, les dirigeants doivent jongler avec une multitude de priorités stratégiques : croissance, innovation, expérience client, conformité, etc.

Pour communiquer efficacement la valeur de l'ingénierie du chaos aux cadres supérieurs, envisagez les approches suivantes :

- Déterminez les principales préoccupations et les principaux facteurs de décision de vos cadres supérieurs.

  Par exemple, les cadres supérieurs s'inquiètent-ils de la perte de clientèle, de la conformité réglementaire, de la réduction des coûts ou des pressions concurrentielles ? Positionnez l'ingénierie du chaos comme un multiplicateur de force adapté aux défis et objectifs uniques de l'entreprise.
- Identifier les objectifs communs et les résultats stratégiques.

  Comment votre stratégie d'ingénierie du chaos soutient-elle la stratégie de croissance globale de l'organisation, l'expérience client, les opportunités de marché et l'efficacité opérationnelle ? Priorisez les initiatives en fonction des objectifs, de l'impact commercial, du retour sur investissement et du risque de ne pas les mettre en œuvre.
- Communiquez l'efficacité de votre stratégie d'ingénierie du chaos en termes quantifiables à l'aide d'indicateurs clés de résilience.

  Commencez par ces quatre indicateurs clés de résilience : disponibilité, délai de détection, temps de réponse et temps de restauration. Associez-les directement aux résultats commerciaux tels que les revenus, les économies de coûts et la réputation de la marque.
- Ne vous perdez pas dans les détails techniques.

Concentrez-vous sur le sentiment général et l'impact commercial mesurable. La haute direction se soucie des résultats qui stimulent la croissance, renforcent la confiance des clients et favorisent l'innovation.

Le paradoxe de la prévention

Lorsque les défauts sont atténués avec succès avant qu'ils ne se manifestent, il devient difficile de convaincre les parties prenantes de la valeur et de la nécessité des mesures préventives prises. Ce phénomène est connu sous le nom de paradoxe de la prévention. Le paradoxe de la prévention est le principal obstacle à l'intégration de l'ingénierie du chaos en tant que nécessité stratégique, et il provient des biais inhérents à la cognition humaine.

Le bogue du passage à l'an 2000 illustre parfaitement ce paradoxe. Des années de préparation et des milliards de dollars ont été investis dans la mise à jour des systèmes informatiques dans le monde entier. Cependant, la transition harmonieuse vers 2000 a été interprétée par beaucoup comme un témoignage du caractère exagéré des préoccupations liées au passage à l'an 2000. Le succès des efforts de prévention entrepris a rarement été reconnu.

Ce paradoxe de prévention continue de représenter un défi pour les entreprises qui investissent aujourd'hui dans l'ingénierie du chaos. Lorsque des pannes potentielles sont évitées avec succès grâce à des mesures proactives, l'absence même de catastrophe peut paradoxalement rendre difficile la justification des ressources consacrées à la prévention.

La cause première de ce phénomène réside dans la façon dont notre esprit est programmé pour traiter l'information. Les processus cognitifs humains visent à réagir aux événements réels et aux résultats visibles et à s'en souvenir. Lorsqu'une catastrophe est évitée, il n'y a aucun récit dramatique à retenir ou à partager. Un autre aspect du paradoxe de la prévention est le biais rétrospectif. Après un non-événement, les individus ont tendance à conclure que rien ne s'est passé, donc ce n'était pas un vrai problème. La possibilité que des précautions appropriées aient permis d'éviter un problème réel n'est pas reconnue. Cet angle mort psychologique représente un défi permanent pour les organisations. Plus vous réussissez en matière de prévention et de résilience, plus vos efforts semblent inutiles rétrospectivement.

Pour remédier au paradoxe de la prévention, votre organisation peut prendre des mesures spécifiques pour rendre le travail invisible de prévention visible, mesurable et valorisé. Les étapes potentielles sont les suivantes :

- Documentez et simulez ce qui aurait pu se passer sans mesures préventives.
- Racontez des événements au cours desquels des mesures préventives ont permis d'éviter des catastrophes potentielles.
- Indiquez les organisations homologues qui ne se sont pas préparées et qui en ont subi les conséquences.
- Présentez les coûts de prévention dans le contexte des impacts potentiels qu'ils préviennent.
- Décomposez les efforts de prévention en étapes et en réalisations visibles.
- Renforcer la mémoire institutionnelle sur les raisons pour lesquelles les mesures préventives existent et sur leur importance historique.
- Sensibilisez régulièrement les parties prenantes à la valeur de la résilience et des pratiques d'ingénierie du chaos.

Conclusion

L'ingénierie du chaos est un impératif stratégique pour les organisations. Bien que votre parcours d'adoption puisse être confronté à des défis tels que des idées fausses, une résistance culturelle et des contraintes de ressources, l'établissement d'objectifs clairs et axés sur le leadership peut catalyser le processus. À mesure que les pratiques mûrissent, quantifiez le retour sur investissement grâce à une approche holistique qui tient compte à la fois des améliorations opérationnelles quantitatives et des avantages organisationnels qualitatifs. L'approche holistique est particulièrement importante en période de tensions économiques.

Pour transformer cette nécessité stratégique en réalité, commencez par évaluer le niveau de maturité actuel de votre organisation. Votre organisation en est-elle au stade de l'expérimentation sur le terrain, à la phase axée sur les objectifs, ou quelque part entre les deux ? Sur la base de cette évaluation, créez une feuille de route personnalisée pour accomplir les tâches suivantes :

- Établissez une gouvernance de l'ingénierie du chaos (par exemple, nommez un responsable de la résilience).
- Intégrez les pratiques du chaos dans les flux de travail de développement.
- Mettre en œuvre des programmes de formation réguliers.
- Développez des mesures de résilience complètes.

Cette transformation ne se fera pas du jour au lendemain. Cependant, la prise de ces mesures concrètes, tout en garantissant le soutien continu de la direction, contribuera à élever l'ingénierie du chaos au même niveau stratégique que la cybersécurité. À l'instar de la cybersécurité, l'ingénierie du chaos peut devenir partie intégrante de l'ADN et des processus opérationnels de votre organisation.

Ressources

- Résultats de l'enquête mondiale ITIC 2021 sur le matériel serveur et la fiabilité des systèmes d'exploitation
- L'argument commercial en faveur de Chaos Engineering
- La cybersécurité en tant qu'investissement stratégique : comment l'optimisation du retour sur investissement peut mener à un avenir plus sûr
- Le guide de l'ingénierie du chaos destiné aux dirigeants d'I&O
- Comment utiliser le score du AWS Resilience Hub
- Mise en œuvre des expériences recommandées à l'aide de la console AWS Resilience Hub

Annexe A – Types d'objectifs pour l'ingénierie du chaos

Les descriptions suivantes des types d'objectifs incluent des exemples concrets de la manière dont Amazon et d'autres organisations ont conçu des objectifs pour l'ingénierie du chaos.

Objectifs d'architecture résiliente

L'un des premiers moteurs de l'adoption de l'ingénierie du chaos est d'identifier et de réduire les points de défaillance uniques (SPOF) dans les systèmes et les infrastructures. Les objectifs sont fixés pour valider la résilience des systèmes et architectures critiques, en particulier pour les nouveaux services ou applications.

Les objectifs d'une architecture résiliente impliquent de mener des expériences de chaos simulant des défaillances dans les dépendances des services. Les expériences confirment si les délais d'attente, les nouvelles tentatives, le comportement de mise en cache et les configurations des disjoncteurs fonctionnent correctement. Ces expériences permettent de découvrir les problèmes à résoudre, évitant ainsi les incidents ayant une incidence sur le client. Par exemple, voir Création de services résilients chez Prime Video grâce à l'ingénierie du chaos.

Objectifs de restauration des services

Les objectifs de reprise des services visent à améliorer la capacité de reprise après une interruption des opérations ou une défaillance de l'infrastructure. Par exemple, votre organisation peut viser à atteindre un objectif de temps de reprise (RTO) spécifique pour vos services principaux en cas de panne. Les équipes peuvent concevoir des expériences de chaos pour valider et optimiser les stratégies d'évacuation, les mécanismes de basculement et les processus de reprise automatisés. Les optimisations réduisent en fin de compte le temps nécessaire à la restauration du service. Pour un exemple, voir AWS Lambda: Résilience under-the-hood.

Objectifs en matière d'expérience utilisateur

Le maintien d'une expérience utilisateur cohérente et fiable est essentiel, en particulier pendant les périodes de forte fréquentation ou d'événements critiques. Dans de tels cas, fixez des objectifs centrés sur la réalisation d'objectifs de niveau de service spécifiques ()SLOs. Cette approche centrée sur le client garantit que les efforts de résilience sont directement liés à la fourniture d'une expérience

utilisateur supérieure, même en cas de panne ou de détérioration des conditions. Par exemple, consultez Engineering Resilience : Lessons from Amazon Search's Chaos Engineering Journey.

Objectifs basés sur des métriques

Vous pouvez définir des objectifs basés sur des indicateurs quantitatifs, tels qu'un score de résilience calculé en attribuant des points aux services qui adoptent les meilleures pratiques éprouvées en matière de résilience. Vous pouvez ensuite utiliser des expériences de chaos particulières pour déterminer le score de résilience. Ce score peut servir de mesure aux équipes pour suivre leurs progrès en matière d'atténuation des risques de disponibilité connus et de mise en œuvre des mesures de résilience recommandées. Cependant, il est essentiel d'interpréter ces scores avec prudence et d'éviter de trop mettre l'accent sur un seul indicateur au détriment d'objectifs de résilience plus larges. Pour un exemple, voir Comprendre les scores de résilience.

Objectifs de conformité réglementaire

Le secteur des services financiers est devenu un acteur de premier plan dans l'adoption de l'ingénierie du chaos, principalement en raison d'exigences réglementaires strictes qui exigent de solides capacités de résilience. Les réglementations exigeront que les institutions financières identifient, testent et corrigent de manière proactive les vulnérabilités de leurs systèmes et processus critiques. Ces réglementations sont notamment les suivantes :

- Le document interinstitutions sur les bonnes pratiques pour renforcer la résilience opérationnelle publié par les agences fédérales américaines
- Les lignes directrices de la Banque centrale européenne en matière de résilience opérationnelle
- La proposition de la Commission européenne pour une loi sur la résilience opérationnelle numérique (DORA)

Si votre organisation est une institution financière, respectez ces réglementations en fixant des objectifs explicites pour démontrer la résilience opérationnelle grâce à des stratégies complètes de test et de validation. Par exemple, voir London Stock Exchange Group utilise l'ingénierie du chaos AWS pour améliorer la résilience.

Annexe B – Mesures quantitatives et qualitatives

Cette section décrit les mesures quantitatives pour suivre les améliorations opérationnelles et les mesures qualitatives pour évaluer les résultats organisationnels généraux issus des pratiques d'ingénierie du chaos.

Mesures quantitatives

Les mesures quantitatives suivantes fournissent un cadre pour le suivi des indicateurs clés qui peuvent démontrer les améliorations opérationnelles et liées aux incidents directs obtenues grâce aux pratiques d'ingénierie du chaos :

- Incidents :
  - Fréquence des incidents – Suivez le nombre d'incidents dans un cadre de classification des incidents et classez-les en fonction de leur criticité (critique, majeur, mineur) sur une période donnée. Pour plus d'informations sur le cadre de classification des incidents, voir l'annexe C.
  - Temps d'arrêt et dégradation – Mesurez la durée totale des interruptions de service ou de la dégradation des services pour chaque catégorie d'incident.
  - Mesures de réponse aux incidents – Pour comprendre les incidents, mesurez le temps de détection, le temps d'identification, le temps d'atténuation, le temps de reprise, le temps d'escalade et d'autres indicateurs connexes pour chaque classification d'incident.
  - Incidents ayant un impact sur le client – Suivez le nombre d'incidents ayant un impact sur les clients ou le pourcentage d'incidents maîtrisés avant l'impact sur le client.
  - Modifications apportées au runbook – Suivez le nombre de mises à jour ou de révisions du runbook résultant des connaissances acquises lors d'expériences sur le chaos. Un manuel d'exécution fournit des instructions détaillées pour effectuer une opération ou une procédure particulière afin de récupérer après un type d'incident particulier.
- Coûts :
  - Coûts d'infrastructure – Collectez des données sur les coûts d'infrastructure, y compris les ressources informatiques en nuage et les mesures de redondance requises par les mesures prises pour améliorer la résilience.
  - Impact sur les clients – Mesurez les impacts sur l'expérience client, les taux de désabonnement et les pertes de revenus associés aux défaillances ou aux temps d'arrêt du système.

  - Productivité du personnel – Suivez le temps consacré par les équipes d'ingénierie et d'exploitation à la réponse aux incidents, à la lutte contre les incendies, à la rédaction d'autopsies et à d'autres tâches réactives liées aux défaillances du système.
- Améliorations continues du système – Comptez le nombre d'améliorations de processus, de modifications architecturales ou de mécanismes de reprise automatisés mis en œuvre en conséquence directe des informations issues d'expériences de chaos.
- Conformité – Suivez les coûts et efforcez-vous de respecter les exigences réglementaires ou les normes du secteur liées à la résilience opérationnelle.
- Adoption – Suivez le taux d'adoption des pratiques chaotiques au sein de l'organisation.
- Satisfaction client – Mesurez l'évolution des indicateurs de satisfaction client pour évaluer l'impact de l'amélioration de la fiabilité du système sur l'entreprise.

Mesures qualitatives

Les mesures qualitatives suivantes fournissent un cadre pour suivre les résultats organisationnels généraux obtenus grâce aux pratiques d'ingénierie du chaos :

- Confiance et préparation des employés :
  - Sondez régulièrement les équipes pour mesurer leur niveau de confiance dans la gestion des incidents du monde réel et leur niveau de préparation perçu aux rotations sur appel.
  - Suivez le pourcentage d'ingénieurs de garde qui ont participé à des expériences de chaos dans le cadre de leur formation.
- Changement culturel :
  - Évaluez dans quelle mesure un état d'esprit de résilience a imprégné l'organisation par le biais d'enquêtes, de sessions de feedback ou d'audits.
  - Suivez le nombre d'équipes qui défendent et défendent activement les pratiques d'ingénierie du chaos.
- Collaboration interfonctionnelle et partage des connaissances :
  - Suivez la fréquence et la participation aux sessions ou ateliers de partage de connaissances entre équipes liés à l'apprentissage de l'ingénierie du chaos.
  - Suivez le nombre d'initiatives conjointes d'ingénierie du chaos impliquant plusieurs équipes ou départements.
- Efficacité de la formation :

  - Évaluez l'efficacité des programmes de formation en ingénierie du chaos en menant des enquêtes ou des évaluations après la formation.
  - Suivez le nombre d'ingénieurs qui participent aux programmes de formation en ingénierie du chaos et lisez les autopsies.
- Attraction et rétention des talents :
  - Évaluez si le programme d'ingénierie du chaos aide à attirer et à retenir les meilleurs talents en ingénierie en réduisant le temps et les efforts consacrés à la réparation des pannes.
- Réputation de la marque :
  - Suivez tout changement dans la perception ou la réputation de la marque lié à l'engagement démontré de l'organisation en matière de résilience opérationnelle.
- Avantage compétitif :
  - Suivez votre avantage concurrentiel par rapport à vos concurrents du secteur en termes de disponibilité des systèmes.

Annexe C – Classification des incidents

Le suivi des incidents au sein d'un cadre de classification est crucial, car celui-ci fournit une vue globale des types de défaillances et des problèmes qui ont un impact sur le système. Si votre organisation ne suit les incidents que dans une seule catégorie, tels que les défaillances d'infrastructure, vous risquez de rater des informations et des opportunités d'amélioration dans d'autres domaines. En suivant les incidents relevant de plusieurs catégories, vous pouvez mieux comprendre la diversité des expériences de chaos à mener. Cette perspective permet d'identifier les angles morts potentiels et d'élargir le champ d'ingénierie, ce qui conduit à un système plus résilient et tolérant aux pannes.

Le cadre de classification des incidents suggéré est conçu pour aider à classer les incidents en fonction de leur nature et de leur impact potentiel. Il utilise une classification de haut niveau qui regroupe les incidents en huit catégories principales :

- Problèmes de déploiement :
  - Déploiements échoués
  - Défaillances liées au rollback
  - Problèmes de configuration lors du déploiement
- Bugs et régressions du logiciel :
  - Bugs fonctionnels
  - Problèmes d'intégration
  - Problèmes de performance
  - Problèmes liés aux quotas
  - Problèmes liés au mécanisme de résilience (nouvelles tentatives, délais d'attente)
  - Problèmes d'intégrité des données
- Problèmes liés aux tests :
  - Tests manquants
  - Tests inefficaces
  - Tests floconneux
- Défaillances de l'infrastructure :
  - Défaillances matérielles (serveurs, périphériques réseau, stockage)
  - Problèmes de dimensionnement

    - Défaillances de dépendance (services tiers, APIs)
    - Problèmes de connectivité réseau
- Problèmes opérationnels :
    - Erreurs humaines (mauvaise configuration, modifications accidentelles)
    - Surveillance et alerte en cas de panne
    - Problèmes liés à la planification des capacités
    - Défaillances de sauvegarde et de restauration
- Incidents de sécurité :
    - Tentatives d'accès non autorisées
    - Violations de données
    - Attaques par déni de service (DoS)
- Pannes de service tiers :
    - Pannes des fournisseurs de cloud
    - Défaillances du DNS
    - Interruptions de service et d'API externes
- Facteurs environnementaux :
    - Catastrophes naturelles (tremblements de terre, incendies, inondations, pannes de courant)
    - Problèmes liés aux conditions météorologiques

Il s'agit d'un exemple de cadre de classification non concluant que vous pouvez adapter à vos besoins spécifiques et à votre organisation. Nous vous recommandons de revoir et de mettre à jour régulièrement le cadre de classification à mesure que votre système évolue ou que de nouveaux types d'incidents apparaissent.

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	—	28 janvier 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 :

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

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

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

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le WQF est inclus avec AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

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

planification de la continuité des activités (BCP)

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

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

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

CCo E

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

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

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

CMDB

Voir base de données de gestion de configuration.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

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

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

administrateur délégué

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

déploiement

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

environnement de développement

Voir environnement.

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

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

reprise après sinistre (DR)

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

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

DR

Voir reprise après sinistre.

détection de dérive

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

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

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

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

époppée

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

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

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

branche de fonctionnalités

Voir succursale.

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le modèle de fondation.

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation des historiens

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

données de rétention

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l'identité

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

application inactive

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

IIo T

Voir Internet industriel des objets.

infrastructure immuable

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

VPC entrant (d'entrée)

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

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

migration incrémentielle

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

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

Internet industriel des objets (IIoT)

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

VPC d'inspection

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

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

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

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

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

zone de destination

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

grand modèle de langage (LLM)

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

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

lift and shift

Voir 7 Rs.

système de poids faible

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

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

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

branche principale

Voir succursale.

malware

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

services gérés

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

système d'exécution de la fabrication (MES)

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

MAP

Voir Migration Acceleration Program.

mécanisme

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

compte membre

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

MAILLES

Voir le système d'exécution de la fabrication.

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

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

microservice

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

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

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

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Voir Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'une organisation dans AWS Organizations. Ce journal de suivi est créé dans

chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les informations personnelles identifiables.

manuel stratégique

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

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

Objet capable de définir les autorisations (voir la politique basée sur l'identité), de spécifier les conditions d'accès (voir la politique basée sur les ressources) ou de définir les autorisations maximales pour tous les comptes d'une organisation dans AWS Organizations (voir la politique de contrôle des services).

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même

technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

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

confidentialité dès la conception

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

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs

VPCs domaines. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices

peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

CHIFFON

Voir Retrieval Augmented Generation.

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Région

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

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

runbook

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

S

SAML 2.0

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

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

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

SPOF

Voir point de défaillance unique.

schéma en étoile

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

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un

exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation AWS Organizations et dans ses comptes en votre nom. Le service de confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir environnement.

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet.

Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir écrire une fois, lire plusieurs.

WQF

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

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité « jour zéro »

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

invite Zero-Shot

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

application zombie

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

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