Élaboration d'une stratégie pour le cloud unique, hybride et multicloud dans le secteur de l'enseignement

AWS Conseils prescriptifs

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Conseils prescriptifs: Élaboration d'une stratégie pour le cloud unique, hybride et multicloud dans le secteur de l'enseignement

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Élaboration d'une stratégie pour le cloud unique, hybride et multicloud dans le secteur de l'enseignement

Amazon Web Services (contributeurs)

Septembre 2023 (historique du document)

Les établissements d'enseignement cherchent à soutenir des fonctions telles que l'apprentissage à distance, la recherche, l'expérience des étudiants, l'analyse des données et l'administration avec l'agilité, les économies de coûts, la sécurité et la résilience qu'offre le cloud computing. De nombreuses entreprises évaluent les déploiements hybrides et multicloud dans le cadre de cette transformation numérique.

Ce paper fournit des conseils prescriptifs sur la création d'une technologie et d'une stratégie de gouvernance uniques, hybrides et multicloud, à l'intention des dirigeants et des décideurs des établissements d'enseignement qui évaluent leurs options cloud. Ces conseils sont basés sur notre expérience de AWS travail avec plus de 14 000 établissements d'enseignement de toutes tailles à travers le monde, des écoles primaires et secondaires à l'enseignement supérieur.

Présentation de

À mesure que les établissements d'enseignement se transforment numériquement pour offrir des services et des expériences différenciés à leurs étudiants, à leurs parents, à leurs professeurs, à leur personnel et à la communauté, ils sont confrontés à une multitude de décisions techniques. De nombreuses entreprises ont déjà pris la décision d'adopter le cloud pour accroître leur agilité, leur élasticité, leur résilience, leur sécurité et leurs économies. Sur la base de leurs relations existantes et de leurs investissements au sein des différentes équipes, la plupart des entreprises utilisent une combinaison de centres de données sur site, d'installations de colocation et de fournisseurs de cloud. Compte tenu de la disponibilité de plusieurs options cloud, les établissements d'enseignement doivent souvent choisir entre des modèles de déploiement uniques, hybrides et multicloud (définis dans la section Stratégies de déploiement du cloud).

Le multicloud, qui consiste à utiliser les services d'au moins deux fournisseurs de services cloud, n'est pas rare pour de nombreuses institutions aujourd'hui. Votre équipe informatique peut préférer un fournisseur de cloud, tandis que d'autres groupes, services ou utilisateurs individuels peuvent choisir ou utilisent déjà d'autres fournisseurs. Les établissements d'enseignement qui ne disposent

pas d'une stratégie claire pour les guider vers le modèle de déploiement cloud approprié rencontrent de nombreux défis. Il s'agit notamment d'une complexité inutile, d'une augmentation des exigences en matière de personnel, d'une gouvernance incohérente et d'approches fondées sur le plus petit dénominateur commun qui les limitent au sous-ensemble des fonctionnalités de base communes à tous les fournisseurs. Chaque défi freine l'innovation et ralentit la transformation numérique.

À l'inverse, si vous disposez d'une stratégie cloud qui vous guide dans l'utilisation d'un cloud unique, hybride ou multicloud, vous pouvez répondre aux exigences de votre mission éducative tout en tirant parti des avantages du cloud d'une manière qui soit durable sur le plan opérationnel pour un succès à long terme. Pour créer cette stratégie, nous recommandons ce qui suit :

- Sélectionnez un fournisseur de cloud principal et stratégique.
- Établissez un centre d'excellence dans le cloud (CCoE).
- Faites la différence entre les applications SaaS (Software as a Service) et les services cloud de base.
- Définissez les exigences de sécurité et de gouvernance pour chaque fournisseur de services cloud.
- Adoptez des solutions gérées natives pour le cloud chaque fois que cela est possible et pratique.
- Mettez en œuvre des architectures hybrides lorsque les investissements existants sur site incitent à une utilisation continue.
- Réservez le multicloud uniquement pour les charges de travail qui ne peuvent pas répondre aux exigences techniques ou commerciales auprès d'un seul fournisseur de cloud.

Ces meilleures pratiques sont décrites en détail dans la section Recommandations de ce paper. Chaque recommandation est importante, mais les priorités de votre établissement dépendront du stade d'adoption du cloud. Par exemple, si vous commencez tout juste à adopter le cloud, concentrez-vous sur la sélection d'un fournisseur cloud stratégique principal, sur l'établissement d'un CCo E et sur l'adoption de solutions gérées natives pour le cloud. Si vous utilisez déjà un seul fournisseur de cloud, concentrez-vous sur l'établissement des exigences fondamentales en matière de sécurité et de gouvernance, et envisagez des architectures hybrides lorsque les investissements dans vos centres de données existants incitent à une utilisation continue. Si votre entreprise fait déjà appel à plusieurs fournisseurs de cloud, concentrez-vous sur la différenciation des applications SaaS et sur la réservation des déploiements multicloud aux rares charges de travail qui en ont réellement besoin.

Table des matières

Stratégies de déploiement dans le cloud

AWS définit le cloud computing comme la fourniture à la demande de ressources informatiques via Internet avec pay-as-you-go tarification. Au lieu d'acheter, de posséder et de gérer des centres de données et des serveurs physiques, vous pouvez accéder à des services technologiques, tels que la puissance de calcul, le stockage et les bases de données, selon vos besoins auprès d'un fournisseur de cloud. Le cloud computing permet aux établissements d'enseignement d'éviter des tâches lourdes indifférenciées telles que l'achat de matériel, la maintenance et la planification des capacités. Lorsque vous adoptez et déployez des solutions cloud, vous pouvez choisir parmi plusieurs modèles : cloud unique, cloud hybride et multicloud.

Cloud unique

Ce modèle n'utilise qu'un seul fournisseur de services cloud. Les applications et les charges de travail mono-cloud peuvent être mises en œuvre directement dans le cloud ou précédemment hébergées dans un autre environnement et migrées vers le cloud. Ces charges de travail peuvent utiliser des services d'infrastructure de niveau inférieur fournis par leur fournisseur de cloud ou tirer parti de services gérés de niveau supérieur. Quoi qu'il en soit, ce modèle adopte un seul fournisseur de cloud et utilise uniquement les services cloud de ce fournisseur.

Cloud hybride

Un modèle de cloud hybride distribue les ressources entre le centre de données sur site d'une entreprise et au moins un fournisseur de services cloud. En général, l'objectif de ce modèle est d'étendre l'infrastructure d'une entreprise dans le cloud tout en maintenant une connectivité privée avec les systèmes internes existants qui résident sur site.

Multicloud

Un modèle multicloud distribue les ressources et utilise les services d'au moins deux fournisseurs de services cloud. Une organisation peut choisir d'opter pour le multicloud, mais le plus souvent, cela est dû au fait que des équipes, des services ou des membres du personnel ont leurs propres préférences pour les différents fournisseurs de cloud.

Recommandations

Maintenant que vous avez une connaissance de base du cloud unique, du cloud hybride et du multicloud, cette section fournit des recommandations détaillées pour le choix d'un modèle.

- Sélectionnez un fournisseur de cloud principal et stratégique
- Établir un CCo E
- Faites la différence entre les applications SaaS et les services cloud de base
- Définissez les exigences de sécurité et de gouvernance pour chaque fournisseur de services cloud
- Adoptez des services gérés natifs dans le cloud chaque fois que cela est possible et pratique
- Mettez en œuvre des architectures hybrides lorsque les investissements existants sur site incitent à une utilisation continue
- Réservez le multicloud uniquement pour les charges de travail qui ne peuvent pas répondre à leurs exigences techniques ou commerciales par le biais d'un seul fournisseur de cloud

Sélectionnez un fournisseur de cloud principal et stratégique

L'adoption du cloud offre de nombreux avantages essentiels à la modernisation informatique, à la rentabilité et à l'innovation. Cependant, l'adoption de technologies cloud allant au-delà des applications SaaS limitées peut présenter des défis que les établissements d'enseignement doivent soigneusement planifier pour éviter des coûts et une complexité inutiles. Les changements technologiques et commerciaux liés à la mise en œuvre des charges de travail dans le cloud nécessitent l'habilitation du personnel et des ajustements de l'infrastructure de base, y compris le réseau, la sécurité, la gouvernance et les opérations.

La meilleure approche pour relever efficacement ces défis, en particulier si votre entreprise en est aux premières étapes de sa transition vers le cloud, consiste à sélectionner un fournisseur de cloud stratégique principal capable de prendre en charge la majorité de vos charges de travail. Commencez par une adoption ciblée centrée sur ce fournisseur afin de simplifier et d'accélérer la concrétisation des avantages du cloud. La sélection d'un fournisseur de cloud principal n'est pas une décision exclusive et irréversible. Il permet à votre entreprise de faire évoluer son adoption du cloud de manière itérative. Vous pouvez commencer par vous concentrer sur quelques services, puis étendre vos activités à d'autres services cloud en fonction des besoins, sans pour autant perdre de vue les avantages globaux du cloud. Cette approche maximise la capacité de votre organisation à tirer parti

des capacités d'un fournisseur, à concentrer et à développer les compétences des employés et les relations avec des partenaires tiers, et à simplifier la gestion des fournisseurs.

Nous avons vu des clients se lancer dans leur transition vers le cloud en essayant d'adopter simultanément plusieurs fournisseurs de cloud, mais nous avons regretté par la suite cette décision et la complexité qu'elle a entraînée. Gartner partage ce point de vue dans son article intitulé 6 étapes pour planifier une stratégie cloud, dont l'étape 2 est « Prioriser un fournisseur principal dans les architectures multicloud ».

Chaque fournisseur de cloud introduit différents modèles d'exploitation et de support, la gestion des identités et des accès, la mise en réseau, les opérations, les capacités de conformité, etc. Il est préférable de maîtriser le modèle d'exploitation d'un fournisseur de cloud à la fois.Vous pouvez ensuite intégrer des services cloud supplémentaires de manière itérative et incrémentielle, lorsque cela est rationalisé. De nombreux facteurs peuvent influencer votre décision d'adopter un fournisseur de cloud principal, mais utilisez les questions clés suivantes pour orienter votre choix.

- Quelle est l'étendue et la profondeur des services proposés par le fournisseur ?

  Les différents fournisseurs de cloud proposent différents services. Assurez-vous au minimum que votre fournisseur principal dispose des capacités nécessaires pour répondre à toutes vos exigences fonctionnelles ainsi qu'à vos besoins opérationnels transversaux tels que la sécurité, la gouvernance et l'automatisation. Sélectionnez un fournisseur qui fournit ces fonctionnalités et qui a fait ses preuves en matière d'innovation et d'excellence opérationnelle. Tenez compte non seulement de vos applications, mais également de vos données. Réfléchissez aux futurs modèles d'intégration et de transfert des données afin de limiter le coût, la latence et la complexité liés au transfert de grandes quantités de données entre fournisseurs. Choisissez un fournisseur qui propose la gamme de services la plus étendue et la plus complète possible pour répondre à vos besoins actuels en matière d'applications et de données, et également pour découvrir de nouveaux cas d'utilisation susceptibles de répondre aux besoins de votre établissement à mesure qu'ils évoluent au fil du temps.
- Le fournisseur peut-il répondre à tous vos besoins en matière de sécurité et de conformité ?

  Dans le secteur de l'éducation, la sécurité et la conformité sont essentielles à tout déploiement technologique. Choisissez un fournisseur de cloud capable de répondre à tous vos besoins en matière de sécurité et de conformité. De tels outils AWS Artifactpeuvent vous aider à évaluer les fournisseurs en proposant une ressource centrale permettant d'accéder à la demande aux rapports de sécurité et de conformité. Tenez compte non seulement de la sécurité et de la conformité de l'infrastructure et des services du fournisseur de cloud, mais également de la facilité avec laquelle

vous pouvez concevoir des solutions sécurisées et conformes à l'aide de ces services. Préférez un fournisseur qui propose une combinaison de solutions prédéfinies, de démarrages rapides et de conseils prescriptifs pour accélérer votre adoption sécurisée du cloud.

- Le fournisseur dispose-t-il d'un solide réseau de partenaires ?

  Aucune entreprise n'entreprend seule une transformation vers le cloud. Pour accélérer l'adoption, vous devez utiliser les services et l'expertise du fournisseur de cloud ainsi que de son réseau de partenaires. Ce réseau comprend des partenaires technologiques qui fournissent des logiciels qui s'exécutent sur, s'intègrent ou prennent en charge la technologie cloud, ainsi que des partenaires consultants qui peuvent vous aider à concevoir, créer, exécuter et gérer vos propres applications dans le cloud. Vous constaterez que de nombreux fournisseurs de technologies éducatives, fournisseurs de logiciels indépendants (ISVs), consultants et revendeurs avec lesquels vous travaillez déjà sont membres du réseau de partenaires du fournisseur de cloud. Privilégiez un fournisseur de cloud disposant du réseau le plus solide de partenaires dotés de compétences éprouvées. Il est essentiel de pouvoir compter sur des partenaires dotés d'une expertise industrielle et technique reconnue.

- Quels sont le support et les moyens proposés par le fournisseur ?

  Pour adopter avec succès toute nouvelle technologie, vous avez besoin de mécanismes permettant de demander de la formation et de l'aide, notamment des recommandations sur les meilleures pratiques, des conseils de configuration et la résolution des problèmes de dépannage. Le choix d'un fournisseur de cloud offrant un support solide et des options de formation vous permettra de réussir. Découvrez le modèle et les ressources d'assistance officiels du fournisseur, ainsi que toutes les ressources tierces ou communautaires disponibles, telles que les blogs, les forums, les vidéos et les guides pratiques. Tenez compte non seulement des programmes de support technique du fournisseur, mais également des programmes axés sur la transformation commerciale et culturelle. Par exemple, le cadre d'adoption du AWS cloud (AWS CAF) aide les entreprises à se transformer numériquement en se concentrant sur des points de vue qui incluent les processus métier et les personnes, et pas seulement la technologie. Préférez un fournisseur de cloud qui propose des options de formation étendues ainsi qu'un modèle de support et une communauté éprouvés et fiables.

Établir un CCo E

Envisagez de faire évoluer votre fonction de direction du cloud par le biais d'un bureau de transformation ou d'un centre d'excellence cloud (CCoE). A CCo E développe et préconise une

approche pour la mise en œuvre de la technologie cloud à grande échelle au sein d'une organisation. Pour une adoption réussie du cloud, concevez votre CCo E de manière à inclure des représentants capables de parler au nom des équipes et des services concernés. Commencez modestement et faites évoluer progressivement le CCo E pour répondre à vos besoins au fur et à mesure que vous progressez dans le processus de transformation. Les représentants de votre principal fournisseur de cloud, tels que votre responsable de AWS compte et votre architecte de solutions, peuvent vous fournir des ressources pour vous guider dans la création de votre CCo E. Un CCo E accélère votre capacité à acquérir une expertise en la matière, à obtenir l'adhésion, à gagner la confiance au sein de votre organisation et à établir des directives efficaces pour répondre aux exigences de votre mission. Il n'existe pas de structure organisationnelle unique qui fonctionne pour toutes les institutions, mais les questions suivantes vous aideront à concevoir votre propre CCo E.

- Qui devriez-vous inclure dans votre CCo E ?

  À sa création, un CCo E pouvait n'inclure qu'une poignée de premiers utilisateurs et de champions du cloud. Le CCo E peut rester faible, mais il devrait évoluer pour inclure des champions capables de défendre à la fois les fonctions commerciales et les fonctions techniques touchées par l'adoption du cloud. Les fonctions commerciales incluent la gestion du changement, les exigences des parties prenantes, la gouvernance, la formation, les achats et les communications. Ces fonctions sont généralement représentées par des membres des équipes administratives et pédagogiques de votre établissement. Les fonctions techniques incluent l'infrastructure, l'automatisation, les outils opérationnels, la sécurité, les performances et la disponibilité. Ces fonctions sont généralement représentées par des membres des équipes informatiques de votre établissement. L' CCoE devrait également chercher à impliquer des fournisseurs et des partenaires, si nécessaire, pour fournir une expertise en la matière. Le CCo E est une organisation vivante. Sa composition, sa forme et sa fonction changeront probablement au fil du temps, et il pourrait même se dissoudre à un moment ou à un autre de sa maturité future.
- Comment l' CCoUE interagit-elle avec ses parties prenantes ?

  Le CCo E est au service d'autres équipes et vise uniquement à informer et à permettre une adoption réussie du cloud. Envisagez d'intégrer des parties du CCo E dans divers départements, écoles et fonctions. Cela permet d'accéder à un plus large éventail de ressources et d'accélérer le feedback interne. Concentrez-vous sur l'établissement de partenariats et sur l'ouverture de voies de communication entre les parties prenantes dès le début afin d'établir la confiance au sein de l'institution et de briser les silos organisationnels. L' CCoE aurait dû définir des mécanismes pour communiquer avec les parties prenantes, recueillir des commentaires et former les utilisateurs. Les indicateurs de réussite du CCo E devraient refléter cette collaboration et cette communication.

Si une équipe est évaluée uniquement en fonction du développement de technologies, d'autres technologies seront créées, mais leur utilisation et leurs résultats ne seront pris en compte qu'après coup. Vos indicateurs devraient plutôt mesurer des éléments tels que le nombre d'équipes qui deviennent autonomes grâce au travail du CCo E, le nombre de fois où le CCo E se trouve sur la voie critique pour les initiatives, le nombre d'événements de formation organisés ou l'ampleur de l'adoption des résultats du CCo E. Un CCo E bien construit et fiable peut être un tremplin vers une transformation organisationnelle plus large fondée sur la confiance.

- Comment établir un CCo E ?

  La plupart des entreprises commencent leur adoption du cloud par des projets pilotes spécifiques et ciblés. Établissez un CCo E dans le cadre de ces projets. Un bon départ est essentiel pour garantir le succès de l'ensemble du voyage.

  - Commencez par un problème commercial. La technologie au service de la technologie est une mauvaise stratégie. Si vous expérimentez des technologies cloud, identifiez un cas d'utilisation commerciale convaincant, aussi petit soit-il. Ensuite, reprenez ce cas d'utilisation pour définir des objectifs clairs sur la manière dont la technologie peut vous aider. N'implémentez pas la solution dans un silo. Prenez en compte les contributions constantes des parties prenantes de l'entreprise avant et pendant la mise en œuvre du projet. Tous les projets cloud réussis reposent sur une étroite collaboration avec les unités institutionnelles qui utiliseront la technologie.
  - Commencez petit. Choisissez un projet à faible risque doté d'une porte bidirectionnelle. Cela signifie que le projet est réversible et que les erreurs peuvent être corrigées rapidement. Les projets pilotes sont entièrement axés sur l'expérimentation. En évitant les projets à haut risque et à grande échelle, vous pouvez mieux contrôler la mise en œuvre et les résultats. Cela permet de cibler des problèmes spécifiques et définissables plutôt que des objectifs généraux. Par exemple, si l'automatisation est l'objectif ultime, essayez d'automatiser des tâches spécifiques plutôt que des tâches complètes.
  - Définissez et mesurez le résultat. Définissez des mesures claires pour évaluer l'avancement et les performances de chaque projet. Définissez l'état final souhaité bien à l'avance afin d'éviter que les attentes des parties prenantes ne soient inégales. Travaillez en étroite collaboration avec les parties prenantes de l'entreprise et les autres dirigeants de l'organisation pour définir les attentes et les gains mesurables. Il est également important de traduire les résultats dans un langage non technique. Parlez en termes d'objectifs institutionnels, tels que la façon dont le projet a amélioré la rétention et réduit le taux de désabonnement, comment il a réduit les coûts et augmenté la rapidité de livraison, etc.

- Commencez par la zone de confort. Choisissez un projet dans un domaine que votre établissement connaît bien. De cette façon, vous pouvez vous assurer que le projet a des objectifs significatifs et compréhensibles avec un impact réel. Un tel projet renforcera la confiance et aura de meilleurs résultats à long terme pour votre organisation. Par exemple, si vous possédez déjà une expertise en analyse de données, vous pouvez démarrer votre transition vers le cloud tout en tirant parti de vos compétences existantes en commençant par un projet d'analyse. Chaque institution possède une expertise différente et doit trouver ses composants uniques pour élaborer une stratégie de transformation numérique réussie.

Faites la différence entre les applications SaaS et les services cloud de base

La plupart des établissements d'enseignement ont déjà adopté des applications SaaS (Software as a Service). Le SaaS fournit à votre établissement une solution complète qui est gérée et gérée par le fournisseur de services. Les applications SaaS les plus courantes incluent les applications de productivité telles que le traitement de texte et le courrier électronique, mais des options SaaS existent également pour de nombreuses charges de travail critiques telles que le progiciel de gestion intégré (ERP), les systèmes d'information des étudiants (SIS) et les systèmes de gestion de l'apprentissage (LMS). Lorsque votre établissement adopte une offre SaaS, votre équipe informatique n'a pas à se soucier de la maintenance du service ou de la gestion de l'infrastructure : vos utilisateurs consomment simplement le service. Ce modèle de prestation réduit la charge de gestion de votre personnel informatique. De nombreuses institutions choisissent d'adopter une approche « SaaS d'abord » dans leur stratégie informatique, en particulier si leurs équipes informatiques ne disposent pas du temps, des ressources ou des compétences nécessaires pour auto-héberger suffisamment la même application. Même si vous disposez des ressources nécessaires pour vous auto-héberger, il peut être plus rentable d'adopter une solution SaaS et d'investir dans d'autres projets.

Lorsque vous utilisez des applications SaaS, votre équipe informatique n'a pas à gérer l'infrastructure sous-jacente. L'endroit où le fournisseur héberge l'application (centre de données sur site, votre fournisseur de cloud principal ou un autre fournisseur de cloud) devient donc moins important. Après avoir choisi un fournisseur de cloud stratégique principal, vous pouvez choisir d'utiliser une offre SaaS hébergée chez un autre fournisseur de cloud ou sur site, dans le centre de données du fournisseur. À l'inverse, même si vos applications SaaS sont hébergées chez un fournisseur de cloud, vous pouvez choisir un autre fournisseur de cloud principal et stratégique en fonction de la capacité de ce fournisseur pour vos charges de travail non SaaS. La distinction entre les

environnements d'hébergement est moins importante pour le SaaS que pour les applications auto-hébergées. Cependant, vous devez toujours tenir compte des questions clés suivantes lorsque vous évaluez la manière dont le SaaS s'intègre au cloud dans le cadre de votre stratégie informatique.

- L'application SaaS est-elle hautement disponible et évolutive ?

  De nombreux fournisseurs ont déjà pris la décision d'adopter le cloud pour leurs offres SaaS. Ce faisant, le fournisseur est en mesure de tirer parti des avantages du cloud en termes de disponibilité et d'évolutivité accrues. En outre, étant donné que le fournisseur peut adopter le modèle de responsabilité partagée du cloud au lieu de gérer et de maintenir une infrastructure physique, il peut investir davantage de temps et de ressources dans la fourniture de nouvelles fonctionnalités. En raison de ces avantages, vous devriez préférer les fournisseurs qui privilégient le cloud et proposent des solutions hébergées dans le cloud.
- L'application SaaS peut-elle répondre à vos exigences de sécurité ?

  Lors de l'évaluation du SaaS, il est important de savoir quelles données l'application stocke, comment elles sont utilisées et quels contrôles de sécurité sont en place pour protéger ces données. Bien que vous n'ayez pas le contrôle direct du stockage des données comme vous le feriez dans votre propre environnement auto-hébergé, vous devez vous assurer que le fournisseur dispose de mécanismes et de contrôles pour gérer vos données de manière appropriée. Sachez quelles fonctionnalités de sécurité sont intégrées à la solution SaaS et quelles fonctionnalités nécessitent une configuration supplémentaire. Le cloud permet aux fournisseurs de SaaS de créer des solutions plus disponibles et évolutives, et ils peuvent également créer des solutions plus sécurisées grâce au modèle de responsabilité partagée. Vous devriez préférer les fournisseurs qui tirent parti des outils et services de sécurité du cloud dans le cadre de leurs solutions.
- À qui appartiennent les données des applications SaaS et comment y accéder ?

  Lorsque vous utilisez le SaaS, vous faites confiance au fournisseur pour gérer correctement les données de votre établissement. N'oubliez pas de consulter les conditions de service et les accords de niveau de service pour les applications SaaS afin de comprendre les facteurs déterminants tels que la propriété, la disponibilité et la durabilité des données. Évaluez les mécanismes de sauvegarde ou d'exportation de vos données ; ils sont particulièrement importants si vous décidez de changer de fournisseur ou si le fournisseur cesse ses services.
- Vos autres services et applications auto-hébergées peuvent-ils s'intégrer à l'application SaaS, quel que soit l'environnement ?

Lors de l'adoption d'une solution SaaS, il est facile de supposer que les services et applications partageant le même environnement d'hébergement (c'est-à-dire les applications utilisant le même fournisseur de cloud ou le centre de données du même fournisseur) bénéficieront d'une intégration plus fluide. Cependant, la plupart des solutions SaaS offrent aujourd'hui une large prise en charge des API et des intégrations tierces. Ne vous limitez donc pas aux solutions hébergées dans le même environnement. Si les intégrations nécessaires existent, il n'est pas nécessaire que les solutions partagent le même environnement sous-jacent. Imaginons par exemple que vous utilisiez une solution SaaS telle que Google Drive ou Microsoft OneDrive pour le stockage de fichiers étudiants dans le cloud. Pour fournir des bureaux virtuels et un streaming d'applications à vos étudiants, vous pouvez déterminer qu'Amazon WorkSpaces Applications est la solution la mieux adaptée à vos besoins. Bien que ces services s'exécutent dans des environnements différents, WorkSpaces Applications possède des intégrations natives avec Google Drive et Microsoft OneDrive, afin que vos étudiants puissent continuer à utiliser leur espace de stockage existant.

- L'application SaaS prend-elle en charge la gestion centralisée des identités ?

  Pour éviter à votre équipe informatique d'avoir à gérer des magasins d'identités disparates et à vos utilisateurs d'avoir à mémoriser plusieurs ensembles d'informations d'identification, assurez-vous que vos solutions SaaS prennent en charge l'intégration avec vos solutions de gestion des identités ou d'authentification unique existantes. La gestion fragmentée des identités réduit la productivité et peut entraîner de mauvaises pratiques de sécurité, telles que l'augmentation des privilèges et la faiblesse des mots de passe. Si la solution SaaS de votre choix ne prend pas en charge l'authentification unique ou votre magasin d'identité existant, déterminez si la valeur commerciale de l'adoption de la solution l'emporte sur la charge de travail accrue pour les utilisateurs et le personnel.
- Comment sécuriser les communications réseau avec l'application SaaS ?

  Dans certains cas, vous aurez peut-être besoin d'une application auto-hébergée pour communiquer avec une application SaaS. Généralement, ces communications seront sécurisées par APIs des mécanismes d'authentification et d'autorisation appropriés. Toutefois, selon les environnements d'hébergement des deux applications, des mécanismes alternatifs ou supplémentaires peuvent être nécessaires pour simplifier ou sécuriser cette communication. Par exemple, si vous hébergez vous-même une application auprès d'un fournisseur de cloud et que vous devez l'intégrer à une application SaaS hébergée sur le même fournisseur de cloud, le fournisseur peut proposer plusieurs options de connexion. Vous pouvez peut-être utiliser des connexions de peering spécifiques au cloud, des interfaces privées ou privées APIs, par exemple AWS PrivateLinkpour empêcher cette communication de traverser l'Internet public. De même,

si votre application sur site dispose d'une connexion réseau dédiée à un fournisseur de cloud via un service tel que AWS Direct Connect, vous pouvez utiliser cette même connexion pour communiquer avec des applications SaaS hébergées sur le même fournisseur de cloud.

Définissez les exigences de sécurité et de gouvernance pour chaque fournisseur de services cloud

Les établissements d'enseignement doivent atteindre divers objectifs en matière de conformité, de gouvernance et de cybersécurité. Le fait de ne pas atteindre ces objectifs peut inclure une perte de réputation institutionnelle, des amendes, des rançons, des violations de données sensibles, le vol de propriété intellectuelle et la dégradation ou la perte complète de fonctions critiques. Grâce au modèle de responsabilité partagée, les institutions qui adoptent des services cloud peuvent réduire la charge administrative en déléguant une partie de la responsabilité de la sécurité de l'infrastructure au fournisseur de services cloud. En outre, vous pouvez bénéficier de services de sécurité conçus spécialement pour le cloud qui offrent des fonctionnalités souvent indisponibles, difficiles à gérer ou dont le coût est prohibitif dans le cadre d'un déploiement sur site. Les exemples incluent des services tels que AWS WAFla protection des applications Web, AWS Shieldla protection par déni de service (DDoS) distribué et Amazon GuardDuty pour la détection des menaces. Une stratégie efficace de sécurité et de gouvernance du cloud permet aux équipes informatiques et de sécurité de se concentrer sur la création de systèmes sécurisés dès la conception, aide l'établissement à s'adapter rapidement à l'évolution des exigences de ses missions et fournit aux professeurs et aux chercheurs des environnements sécurisés pour un apprentissage et une innovation révolutionnaires. Pour évaluer vos exigences en matière de sécurité et de gouvernance, posez-vous les questions clés suivantes.

- Sur quels cadres de conformité vos charges de travail doivent-elles s'aligner ?

  Les établissements d'enseignement doivent adhérer à de nombreux cadres de conformité en raison de la multitude de parties prenantes et des charges de travail qu'ils supportent. Ces cadres de conformité incluent la Family Educational Rights and Privacy Act (FERPA), la Health Insurance Portability and Accountability Act (HIPAA), le Federal Risk and Authorization Management Program (FedRAMP), la certification du modèle de maturité en matière de cybersécurité (CMMC), l'International Traffic in Arms Regulations (ITAR), les Criminal Justice Information Services (CJIS) et la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS). Dans certains cas, comme dans le cas du CMMC, les subventions de recherche ne sont pas débloquées tant que les charges de travail pertinentes ne sont pas certifiées conformes. Chaque framework

est unique et peut s'appliquer uniquement à un sous-ensemble de charges de travail. Assurez-vous de savoir quelles charges de travail doivent respecter quelles exigences et que vous êtes en mesure de répondre à ces exigences dans l'environnement de chaque charge de travail. Dans les environnements cloud, assurez-vous de bien comprendre vos responsabilités par rapport aux responsabilités du fournisseur de cloud. Vous devez disposer des connaissances, des ressources et des compétences nécessaires pour atteindre et maintenir la conformité.

- Quels mécanismes avez-vous mis en place pour garantir la conformité de plusieurs fournisseurs de cloud sans entraver l'innovation ?

  Si votre établissement universitaire découvre le cloud pour la première fois, nous vous recommandons de sélectionner un fournisseur de services cloud stratégique principal et de vous concentrer sur la compréhension de la manière de concevoir, de concevoir et d'exploiter des environnements cloud sécurisés dès la conception. Idéalement, les contrôles de sécurité intégrés automatiquement dans les systèmes en libre-service permettent aux utilisateurs de déployer rapidement des environnements cloud sécurisés avec un minimum d'intervention de la part des équipes informatiques. En vous concentrant sur un seul fournisseur, vous limitez les ressources et le temps que vous devez investir pour garantir la sécurité et la conformité. Les institutions les plus performantes choisissent un fournisseur de services cloud capable de répondre à la majorité des exigences de conformité, de disposer d'un solide réseau de partenaires, de proposer des solutions de conformité prédéfinies et de proposer une automatisation sécurisée en libre-service. Si vous devez garantir la sécurité et la conformité de plusieurs fournisseurs de cloud, des investissements supplémentaires seront nécessaires pour développer les compétences et les ressources nécessaires à la gestion de la conformité pour chaque environnement. Si chaque fournisseur de cloud utilise un environnement fondamental ou une zone d'atterrissage différent, vous devez comprendre quelles normes et exigences de conformité chaque zone d'atterrissage peut prendre en charge, ce qui peut déterminer si certaines charges de travail peuvent être hébergées chez ce fournisseur. Vous pouvez gérer la conformité pour chaque fournisseur séparément ou utiliser des solutions personnalisées ou partenaires qui peuvent centraliser la gestion entre les fournisseurs. AWS Marketplacefournit des solutions clé en main qui peuvent également répondre à vos exigences de conformité.
- Comment pouvez-vous évaluer et contrôler les coûts et l'utilisation de plusieurs fournisseurs de cloud ?

  Si votre établissement universitaire utilise le cloud pour la première fois, nous vous recommandons de mettre en place des mécanismes de visibilité et de contrôle des coûts afin de savoir quels services cloud sont utilisés, à qui appartiennent les ressources cloud, quel est l'objectif de

ces ressources cloud et quelles économies potentielles peuvent être réalisées en optimisant la consommation. Les institutions peuvent obtenir un retour sur investissement significatif en s'associant à leur fournisseur de services cloud pour migrer et moderniser les systèmes critiques, car elles peuvent négocier des accords au niveau de l'entreprise, bénéficier d'une tarification en volume et tirer parti de l'expertise du fournisseur de services cloud. Si vous devez contrôler les coûts et l'utilisation de plusieurs fournisseurs, réfléchissez à la manière dont vous pouvez agréger et analyser les coûts et l'utilisation de chaque fournisseur, soit à l'aide de processus et d'outils internes, soit en utilisant des solutions partenaires. De nombreuses organisations commencent à identifier les opérations financières dans le cloud (FinOps) comme une fonction clé et à consacrer des ressources à l'évangélisation et à la mise en œuvre de capacités de gestion et d'optimisation des coûts du cloud.

- Disposez-vous de mécanismes permettant de gérer facilement les autorisations des utilisateurs au fil du temps ?

  Nous recommandons aux établissements universitaires de comprendre les principaux besoins des parties prenantes lorsqu'ils abordent le cloud pour la première fois. Les utilisateurs des systèmes institutionnels incluent les étudiants, les professeurs, les chercheurs, le personnel informatique, l'administration, la sécurité, le grand public et les collaborateurs tiers. Vous devez identifier les besoins fondamentaux de ces utilisateurs et vous assurer que les mécanismes appropriés sont en place pour leur accorder l'accès aux services cloud. Les différents types d'utilisateurs ont besoin de différents types d'accès aux services cloud. Par exemple, les étudiants, les professeurs et le grand public doivent avoir accès aux applications ; le personnel informatique, les administrateurs et les responsables de la sécurité doivent avoir accès à une infrastructure cloud ; les chercheurs et leurs collaborateurs tiers doivent avoir accès à des environnements de recherche sécurisés ; les professeurs doivent avoir accès à des environnements d'enseignement sécurisés et peuvent même vouloir fournir aux étudiants un accès pratique aux technologies cloud. Vous devez disposer d'outils pour gérer ces identités de manière centralisée et automatisée, et utiliser les processus établis pour identifier, accorder et révoquer les autorisations à mesure que les rôles et les responsabilités évoluent au fil du temps.
- Avez-vous mis en place des mécanismes pour intégrer de manière appropriée les nouveaux systèmes à votre solution de gestion des identités ?

  Nous recommandons aux établissements universitaires de faciliter l'intégration de nouveaux systèmes à leurs systèmes de gestion des identités. Cela donne à l'institution la flexibilité nécessaire pour prendre en charge diverses fonctions critiques en permettant aux parties prenantes de se procurer et de créer des systèmes qui peuvent être facilement intégrés dans le

système de gestion des identités. En simplifiant le processus d'intégration, les parties prenantes seront moins enclines à utiliser leurs propres mesures de contrôle d'accès, qui risquent de ne pas appliquer les meilleures pratiques de sécurité telles que l'authentification unique, les clés d'accès et l'authentification multifactorielle (MFA). Assurez-vous que votre système de gestion des identités peut interagir avec les systèmes nécessaires par le biais d'intégrations natives ou de protocoles conformes aux normes du secteur.

- Disposez-vous de mécanismes permettant une détection et une réponse efficaces aux incidents ?

  Les établissements d'enseignement sont fréquemment la cible de cyberattaques et de ransomwares. Pour aider à détecter et à répondre efficacement à de tels incidents, nous recommandons une approche bifurquée :

  - Concentrez vos efforts sur les mesures préventives sous la forme de contrôles de sécurité intégrés automatiquement dans les environnements cloud.
  - Mettez en œuvre des fonctionnalités de détection qui aident les intervenants en cas de cyberincident à détecter, contenir et atténuer les failles de sécurité en temps opportun.

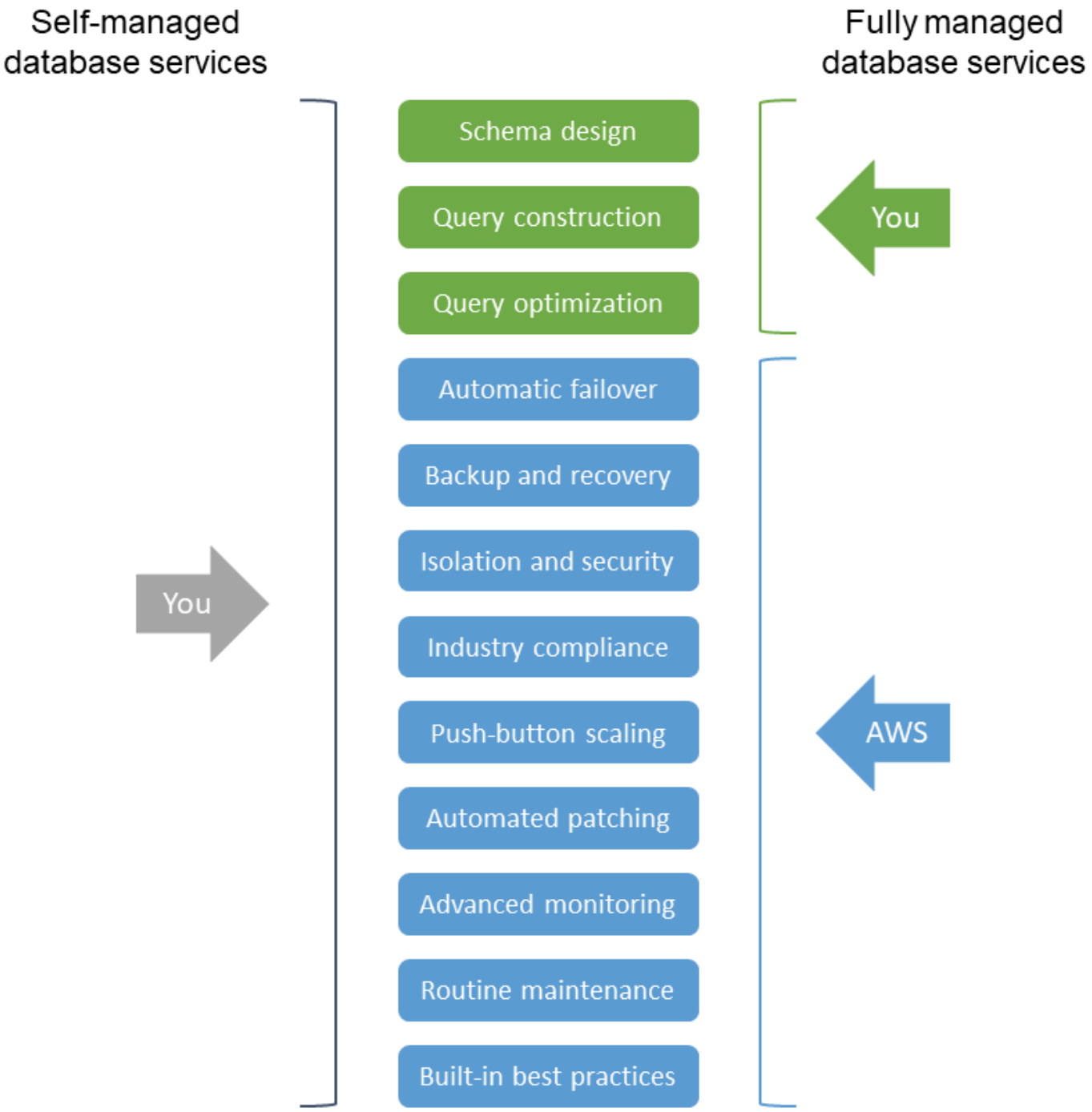
Comme pour la conformité, vous devez vous assurer de disposer des ressources, des compétences et des outils nécessaires pour détecter, prévenir et répondre aux événements dans chaque environnement. En vous concentrant sur un seul fournisseur de cloud principal, vous pouvez limiter les ressources nécessaires. Les établissements universitaires qui ne disposent pas d'une équipe responsable des opérations de sécurité devraient faire appel à des fournisseurs de logiciels indépendants, à des fournisseurs de solutions gérées de détection et de réponse et à des consultants en cybersécurité pour obtenir de l'aide dans ces domaines.

Adoptez des services gérés natifs dans le cloud chaque fois que cela est possible et pratique

Lorsque vous réfléchissez initialement à la manière de tirer parti des services cloud, l'utilisation de services d'infrastructure et d'outils de développement familiers à vos équipes peut sembler être la meilleure solution. Cependant, le choix de services gérés natifs dans le cloud, en particulier les options sans serveur, peut considérablement réduire les coûts, les efforts et la complexité.

Les services gérés natifs du cloud éliminent de nombreuses tâches informatiques indifférenciées qui nécessitent du temps et des efforts de la part de votre personnel, qui pourraient être mieux consacrés à des activités axées sur la mission. En outre, à mesure que les fournisseurs améliorent les capacités de leurs services, vos solutions héritent naturellement d'améliorations progressives en termes

d'efficacité, de sécurité, de résilience, de performance et d'autres caractéristiques. Par exemple, un service de base de données entièrement géré est un système de gestion de base de données relationnelle riche en fonctionnalités, mais il n'est pas nécessaire de configurer ni de gérer le serveur et le système d'exploitation sous-jacents sur lesquels la base de données s'exécute. Cela élimine les tâches administratives généralement requises lorsque vous gérez une base de données relationnelle dans votre propre centre de données ou sur un serveur virtuel autogéré que vous approvisionnez dans le cloud. Le schéma suivant illustre cette différence.



Les avantages de l'élimination de la gestion de l'infrastructure sont évidents lorsque vous comparez un service géré natif du cloud à une approche autogérée comparable. Par conséquent, chaque fois que vous devez déployer des composants sur lesquels vos applications achetées ou développées sur mesure seront exécutées, vous devez utiliser des services gérés natifs pour le cloud afin de réduire le temps et les efforts.

Lorsque votre équipe est chargée de créer, de déployer ou de gérer des solutions dans le cloud, utilisez des services gérés natifs pour le cloud afin de tirer pleinement parti des capacités et des innovations différenciées de votre fournisseur de cloud. Cette stratégie vous permet de sélectionner, d'intégrer et de déployer des services cloud de manière à réduire le temps et les efforts nécessaires à ces projets, tout en augmentant leur résilience et leur sécurité. Pour une stratégie cloud réussie, envisagez d'adopter ces éléments de base natifs pour le cloud lorsque vous migrez des solutions personnalisées vers le cloud, développez de nouvelles solutions dans le cloud ou déployez des logiciels sous licence sur le cloud. Lorsque vous évaluez les options de services gérés natifs du cloud, posez-vous les questions clés suivantes.

- Devez-vous consacrer une plus grande partie du temps et des efforts de votre personnel aux fonctionnalités qui sont au cœur de votre mission éducative ?

  La gestion des serveurs, même virtuels, demande du temps et de l'attention pour garantir qu'ils restent à jour avec les mises à jour logicielles et les correctifs du système. L'utilisation de services gérés qui gèrent ces tâches à votre place vous permet de consacrer le temps du personnel informatique à des activités qui correspondent plus directement à la mission de votre établissement. Par exemple, si vous devez déployer des conteneurs, envisagez un service géré sans serveur, AWS Fargateafin de ne pas avoir à configurer et à gérer des serveurs. En éliminant le besoin d'acquérir, de provisionner et de gérer l'infrastructure sous-jacente, vous pouvez vous concentrer sur la fourniture de nouvelles fonctionnalités, l'optimisation des performances et l'amélioration de l'expérience utilisateur. Tenez compte de cet avantage lorsque vous évaluez les services gérés par rapport aux options autogérées.
- Quels efforts faudra-t-il à votre équipe pour adopter des services gérés natifs dans le cloud ?

  La conception et la mise en œuvre de solutions utilisant des services gérés natifs pour le cloud peuvent nécessiter un certain apprentissage, mais ces efforts seront récompensés par une réduction des coûts, du temps et de la complexité au cours de la durée de vie d'une solution. En raison de la pay-as-you-go nature à la demande du cloud computing, les services cloud natifs vous permettent d'itérer rapidement et d'expérimenter de manière plus agile tout en évitant les investissements initiaux. Cela se traduit par une innovation accrue et des délais de projet plus courts. Toutefois, pour tirer efficacement parti de ces avantages, réfléchissez à ce qui pourrait être nécessaire pour adopter et utiliser le service, comme la formation du personnel sur les modèles d'utilisation optimaux et la refactorisation du code pour répondre aux besoins spécifiques du service. APIs Même si le service utilise les normes du secteur ou l'open source APIs, vous devrez peut-être refactoriser ou configurer votre application pour gérer les disparités entre les fonctionnalités ou les incohérences entre les versions.

- Comment déployez-vous et gérez-vous actuellement l'infrastructure ? Devez-vous maintenir ce niveau de contrôle ?

  Il existe différentes manières d'héberger et de gérer l'infrastructure dans le cloud, notamment en utilisant des hôtes bare metal, des machines virtuelles, des services de conteneurs gérés et des offres sans serveur. Même si vous utilisez actuellement une infrastructure similaire, telle que des machines virtuelles ou des conteneurs, dans votre environnement sur site, déterminez si une autre approche serait adaptée à certaines charges de travail. Par exemple, au lieu d'exécuter toutes les applications sur des machines virtuelles, envisagez de conteneuriser vos applications et de tirer parti des services de conteneurs gérés tels qu'Amazon Elastic Container Service (Amazon ECS). Cela peut nécessiter une refactorisation, mais vous pouvez utiliser un outil tel que AWS App2Containerpour simplifier et faciliter la conteneurisation. Pour aller encore plus loin, au lieu de déployer des serveurs ou des conteneurs pour tous les composants, envisagez des options entièrement sans serveur. Les technologies sans serveur proposent une mise à l'échelle automatique, une haute disponibilité intégrée et un modèle pay-for-use de facturation pour accroître l'agilité et optimiser les coûts. Dans le même temps, ils éliminent le besoin de gérer les serveurs et de planifier la capacité. Les services informatiques sans serveur tels que ceux qui AWS Lambdasont au cœur des architectures sans serveur. Lambda prend en charge les langages de programmation courants et permet aux développeurs de se concentrer sur le code des applications plutôt que sur la gestion de l'infrastructure. Explorez ces options pour chaque charge de travail et prenez en compte des facteurs tels que la courbe d'apprentissage, les frais de gestion, les coûts et les licences.
- Devez-vous déployer et gérer l'infrastructure d'un logiciel sous licence ?

  Lorsque vous déployez et gérez des logiciels sous licence auprès de fournisseurs de logiciels indépendants (ISVs), il peut sembler logique d'imiter votre déploiement sur site avec une infrastructure cloud. Par exemple, vous pouvez envisager de remplacer les machines virtuelles sur site par des machines virtuelles hébergées dans le cloud. Bien qu'il s'agisse d'une option viable, déterminez si vous pouvez remplacer certains composants de l'architecture par des services gérés natifs pour le cloud. Par exemple, vous pouvez remplacer un serveur de base de données autogéré par un service de base de données entièrement géré qui réduit la charge administrative tout en exécutant le même moteur de base de données. Beaucoup utilisent ISVs déjà des architectures cloud qui tirent parti des services gérés et peuvent même proposer des modèles prédéfinis pour simplifier le déploiement. Dans la mesure du possible, vous devriez préférer ISVs des conseils prescriptifs et une assistance pour les déploiements dans le cloud. Avant de déployer un logiciel sous licence dans le cloud, assurez-vous de consulter votre éditeur

de logiciels pour comprendre en quoi les licences d'environnement cloud peuvent différer des licences sur site.

- Craignez-vous que l'utilisation d'un service géré n'entraîne une dépendance vis-à-vis d'un fournisseur ?

  De nombreux services gérés natifs du cloud sont conçus pour prendre en charge les normes sectorielles courantes et APIs. Par exemple, les services d'analyse tels qu'AWS GlueAmazon EMR sont basés sur des frameworks de traitement et de stockage standard tels qu'Apache Spark et Apache Parquet. AWS Lambdasupporte nativement le code Java, Go, Microsoft PowerShell, Node.js, C#, Python et Ruby. Amazon Relational Database Service (Amazon RDS) prend en charge plusieurs versions de moteurs de base de données courants, notamment SQL Server, Oracle, PostgreSQL et MySQL. Lorsque les services disposent de solutions propriétaires APIs, natives ou partenaires peuvent être disponibles pour interagir avec eux APIs en utilisant des protocoles communs indépendants du cloud. Par exemple, Amazon Simple Storage Service (Amazon S3) dispose d'une API spécifique au service pour une intégration directe, mais vous pouvez également interagir avec celui-ci en utilisant des protocoles de stockage standard tels que le Network File System (NFS), le Server Message Block (SMB) et l'Internet Small Computer Systems Interface (iSCSI) lorsque vous l'utilisez. AWS Storage Gateway Vous devez toujours vous concentrer sur le choix du service géré natif du cloud qui répond le mieux à vos besoins tout en réduisant au maximum les frais d'exploitation, mais vous pouvez préférer les services qui utilisent ou mettent à disposition les normes et protocoles courants du secteur.

Mettez en œuvre des architectures hybrides lorsque les investissements existants sur site incitent à une utilisation continue

La plupart des établissements d'enseignement ont investi dans des centres de données sur site de différentes échelles pour héberger des applications d'entreprise, des solutions de stockage de données, des environnements informatiques pour les utilisateurs finaux (EUC) et des ressources informatiques partagées. Toutes les ressources de ces centres de données sont soumises à des cycles d'actualisation différents, au cours desquels vous devez tenir compte de la croissance future et fournir une capacité suffisante pour faire face aux pics d'échelle, ce qui peut n'être nécessaire que quelques fois par an. Par conséquent, les ressources restent souvent inactives jusqu'au prochain cycle d'actualisation. La planification, la budgétisation, l'achat et le déploiement du nouveau matériel peuvent prendre des semaines, voire des mois, voire plus. Ce long processus freine l'innovation et peut retarder l'apprentissage et la recherche.

Le cloud computing permet de relever bon nombre de ces défis. Le cloud fournit des ressources pay-as-you-go informatiques à la demande, ce qui vous permet de mieux adapter la capacité actuelle aux demandes réelles sans planification ni investissement initiaux importants. Toutefois, si vous avez déjà réalisé un investissement important dans du matériel et des ressources sur site, vous devez chercher à utiliser ces ressources de manière efficace et à les augmenter selon les besoins grâce à la technologie cloud dans un modèle hybride.

Une stratégie de cloud hybride réussie tire parti des investissements existants tout en offrant une agilité, une évolutivité et une fiabilité supérieures à celles que ces investissements peuvent à eux seuls soutenir. Les considérations suivantes peuvent vous aider à démarrer.

- Lorsque vous devez héberger une nouvelle charge de travail, pensez-vous d'abord au cloud ?

  La façon dont vous utilisez conjointement les infrastructures de cloud public et privé définit votre stratégie de cloud hybride. Une approche privilégiant le cloud ne signifie pas que le cloud est le meilleur choix pour toutes vos charges de travail. Toutefois, lorsque vous planifiez de nouvelles charges de travail, considérez le cloud comme première option, en particulier pour les charges de travail qui nécessitent de nouvelles technologies ou qui dépassent la capacité de stockage et de calcul disponible sur site. Les charges de travail dont les modèles d'utilisation sont transitoires et incohérents, qui nécessitent des résultats rapides, qui sont facilement transférables ou qui nécessitent le matériel le plus récent sont des candidats idéaux pour l'évolutivité et l'élasticité du cloud. Déterminez également si la charge de travail bénéficierait de services gérés natifs dans le cloud qui ne sont pas disponibles sur site, même si vous disposez de la capacité disponible.
- Comprenez-vous le coût total de possession de votre environnement sur site et travaillez-vous en partenariat avec votre directeur financier lorsque vous réalisez de nouveaux investissements ?

  Nous vous recommandons de comprendre le véritable coût total de possession (TCO) associé à la maintenance de votre propre centre de données sur site. De nombreux coûts cachés sont associés à la possession et à l'exploitation de l'infrastructure sur site, notamment non seulement le matériel, les logiciels et le support, mais également les installations, les services publics, les assurances et les heures de travail du personnel. Ces coûts peuvent avoir un impact négatif sur la productivité du personnel, la résilience opérationnelle et l'agilité de l'entreprise. Évaluez également vos structures de licence actuelles ainsi que leurs périodes de renouvellement et de maintenance. Le partenariat avec votre directeur financier (CFO) peut vous aider à identifier tous les coûts cachés lorsque vous envisagez de réaliser de nouveaux investissements. Certaines licences peuvent proposer des options BYOL (Bring Your Own License) dans le cloud, ou elles peuvent être plus ou moins propices aux services cloud. Comprendre le coût total de possession réel de votre infrastructure

actuelle vous permet de prioriser l'adoption du cloud pour les charges de travail qui ont le plus d'impact sur le coût total de possession de votre entreprise. L'équipe chargée de votre AWS compte dispose d'outils facilement accessibles pour vous aider à mieux comprendre votre coût total de possession sur site.

- De quelle infrastructure aurez-vous besoin pour prendre en charge les déploiements hybrides ?

  Pour réussir à adopter des modèles hybrides, vous aurez besoin d'outils de base en matière de réseau, de sécurité et d'infrastructure. Assurez-vous de pouvoir maintenir une connectivité réseau adéquate avec votre fournisseur de cloud. Cela peut se faire par le biais d'une combinaison de connectivité Internet existante, de réseaux privés virtuels (VPNs), de connexions dédiées telles que des fournisseurs de connectivité tiers Direct Connect, ou d'Internet2 et de réseaux régionaux de recherche et d'enseignement. Assurez-vous de disposer d'une gestion unifiée des identités et des accès dans vos environnements sur site et dans le cloud. Établissez des outils et des processus pour appliquer des garde-fous cohérents en matière de sécurité, de coûts et d'utilisation.

- Votre personnel informatique est-il prêt à effectuer des déploiements hybrides ?

  Les services cloud peuvent nécessiter des compétences spécifiques que votre équipe ne possède peut-être pas. Pour limiter la formation et les habilitations nécessaires pour améliorer les compétences de votre personnel informatique en vue d'une adoption efficace du cloud, déterminez si le fournisseur de cloud propose des services qui réutilisent et s'appuient sur les compétences existantes sur site et dans le cloud. Par exemple, si vous utilisez et connaissez Kubernetes, vous pouvez envisager d'utiliser Amazon Elastic Kubernetes Service (Amazon EKS) ou Amazon EKS Anywhere. Si vous utilisez et connaissez bien Amazon pour ONTAP NetApp, vous pouvez envisager d'utiliser Amazon FSx pour NetApp ONTAP. De même, déterminez également si les solutions partenaires existantes que vous utilisez disposent d'intégrations natives ou prennent en charge les environnements cloud.

- Pouvez-vous décharger le stockage à long terme ou le calcul à faible utilisation du stockage sur site vers le cloud ?

  Le stockage dans le cloud fournit plusieurs options économiques pour le stockage de données à long terme. Par exemple, Amazon Simple Storage Service (Amazon S3) propose différents niveaux de stockage optimisés pour différents cas d'utilisation. Si votre établissement doit conserver certaines données pendant une longue période, envisagez des solutions de stockage frigorifique telles qu'Amazon Glacier. Le transfert de ces données vers le stockage dans le cloud peut libérer un précieux stockage sur site à hautes performances. Des services tels que AWS Storage Gatewayceux qui permettent aux applications sur site d'accéder facilement aux

niveaux de stockage dans le cloud via des protocoles standard tels que SMB, NFS et iSCSI. De même, envisagez de décharger les tâches informatiques peu ou peu utilisées. Si vous disposez de serveurs sur site dédiés à de telles tâches, vous pouvez plutôt utiliser des services de cloud computing évolutifs, dans lesquels les ressources sont fournies à la demande et vous ne payez que pour ce que vous utilisez. Ces options économiques de stockage à long terme et de calcul à faible utilisation font également du cloud un outil idéal pour la sauvegarde et la reprise après sinistre. Vous pouvez utiliser un stockage et un calcul sécurisés, durables et évolutifs dans le cloud pour protéger vos données et les récupérer rapidement en cas de sinistre sans avoir à maintenir vous-même l'infrastructure de stockage et de calcul nécessaire.

- Disposez-vous d'une capacité suffisante sur place pour expérimenter et innover ?

  Le manque d'élasticité et d'agilité dans les environnements locaux de taille fixe peut limiter les services et les technologies mis à la disposition de vos utilisateurs. Si vos cycles d'actualisation sont stricts, les nouvelles charges de travail devront peut-être attendre le cycle suivant pour être mises en œuvre. Ce modèle opérationnel peut limiter l'expérimentation et ralentir l'innovation. Lorsque vous devez tester une charge de travail nouvelle ou inédite, pensez à utiliser des services cloud évolutifs et élastiques. Les ressources du cloud peuvent être provisionnées et déprovisionnées à la demande et vous ne payez que pour ce que vous utilisez. Vous pouvez ainsi expérimenter et échouer rapidement tout en minimisant les risques organisationnels.

- Avez-vous des exigences de conformité ou de performance uniques qui vous obligent à conserver les données sur site ?

  Les charges de travail soumises à des exigences strictes en matière de résidence ou de latence des données peuvent vous obliger à conserver les données sur site ou aussi près que possible de vos utilisateurs. Pour ces cas d'utilisation, vous pouvez prioriser l'utilisation des ressources locales existantes. Cependant, déterminez si votre fournisseur de cloud propose des services de pointe ou des mécanismes permettant d'utiliser la technologie cloud sur site. Les services Edge assurent le traitement, l'analyse et le stockage des données au plus près de vos propres terminaux et vous permettent de déployer des outils en dehors des centres de données standard des fournisseurs de cloud. Par exemple, AWS propose des services tels que les Zones AWS Locales et permet AWS Wavelengthde déployer des applications dans des lieux spécifiques, plus proches des utilisateurs finaux. Vous pouvez également intégrer des services et des fonctionnalités cloud à votre centre de données existant grâce à des services tels qu'AWS OutpostsAmazon ECS Anywhere et Amazon EKS Anywhere. AWS Storage Gateway

Réservez le multicloud uniquement pour les charges de travail qui ne peuvent pas répondre à leurs exigences techniques ou commerciales par le biais d'un seul fournisseur de cloud

Le multicloud fait référence à l'utilisation de services cloud fournis par plusieurs (deux ou plusieurs) fournisseurs de services cloud. Une stratégie multicloud peut offrir certains avantages, tels que la possibilité de tirer parti des capacités différenciées de plusieurs fournisseurs de cloud ou la capacité de répondre à des exigences de souveraineté des données auxquelles un seul fournisseur de cloud pourrait ne pas être en mesure de répondre. Cependant, pour chaque fournisseur que vous utilisez, assurez-vous de disposer du personnel, des compétences, de la formation et des outils appropriés pour utiliser efficacement ce fournisseur. En outre, si vous souhaitez utiliser une stratégie multicloud pour une charge de travail spécifique, vous aurez besoin de ressources supplémentaires pour intégrer et interopérer les services nécessaires fournis par chaque fournisseur de cloud. Nous vous recommandons de n'envisager le multicloud que lorsque les avantages l'emportent sur l'investissement accru. Pour déterminer si vous devez choisir une stratégie multicloud, posez-vous les questions clés suivantes.

- Disposez-vous des ressources et des compétences nécessaires pour naviguer dans les services proposés par les différents fournisseurs de cloud ?

  Lorsque plusieurs fournisseurs de cloud proposent différents produits et services, votre personnel a besoin de compétences essentielles pour exploiter les capacités de chaque fournisseur. L'utilisation des services d'un seul fournisseur de cloud peut nécessiter le renforcement des compétences et la formation de votre personnel, en fonction des services et des fonctionnalités que vous utilisez. Si vous envisagez une stratégie multicloud, évaluez vos ressources existantes afin de déterminer les compétences supplémentaires dont vous auriez besoin pour utiliser efficacement les services de plusieurs fournisseurs de cloud. Vous devrez peut-être augmenter votre personnel ou investir du temps et de l'argent supplémentaires dans le renforcement des compétences et la formation au-delà de ce qui serait requis pour un seul fournisseur de cloud. Si vous avez déjà des équipes ou des utilisateurs individuels qui utilisent différents fournisseurs de cloud, considérez les avantages organisationnels liés à leur consolidation au sein d'un fournisseur de cloud case-by-case principal.
- Quels frais supplémentaires une architecture multicloud particulière entraînerait-elle ?

  L'un des moteurs courants du multicloud est le désir d'utiliser un service géré spécifique d'un fournisseur dont les capacités peuvent être différenciées des services d'un autre fournisseur de

cloud. Par exemple, vous souhaiterez peut-être utiliser un fournisseur de cloud pour vos besoins d'infrastructure et le service géré d'un autre fournisseur pour les services de domaine et d'annuaire. Cependant, même si ce service géré unique réduit la charge administrative et simplifie la gestion de ce composant d'architecture, il peut entraîner des frais supplémentaires pour d'autres charges de travail, telles que la refactorisation du code, les besoins de connectivité privée ou les tâches d'intégration manuelle. Identifiez ces frais supplémentaires dès le départ et assurez-vous qu'ils ne compensent ni n'éclipsent les avantages que votre équipe peut tirer d'un service différencié.

- Comment centraliserez-vous la surveillance et la gestion entre les fournisseurs de cloud ?

  Lorsque vous commencez à déployer des applications et des fonctionnalités en utilisant les ressources de différents fournisseurs de cloud, réfléchissez à la manière dont vous allez étiqueter, surveiller et gérer ces ressources. Chaque fournisseur disposera de ses propres outils, que vous pourrez peut-être étendre à d'autres environnements. Par exemple, vous pouvez utiliser Amazon CloudWatch pour surveiller les indicateurs et les journaux clés, créer des alarmes et visualiser vos applications et votre infrastructure dans des environnements monocloud, hybrides et multicloud. Vous pouvez également l'utiliser AWS Systems Managerpour améliorer la visibilité et le contrôle des ressources, diagnostiquer et résoudre rapidement les problèmes opérationnels, et automatiser des processus tels que la mise à jour et l'application de correctifs aux machines virtuelles dans tous les environnements. Si vous avez des exigences que les outils d'un fournisseur ne peuvent pas prendre en charge, vous pouvez explorer des solutions partenaires, mais celles-ci peuvent entraîner des coûts supplémentaires ou des efforts d'intégration supplémentaires.
- Comment gérer l'infrastructure sous forme de code avec automatisation lorsque vous utilisez différents fournisseurs de cloud ?

  Lorsque vous gérez des ressources dans le cloud, le provisionnement et la gestion automatisés des ressources vous aident à gérer efficacement différents environnements. Les outils d'automatisation APIs et les outils d'automatisation natifs varient selon les fournisseurs de cloud. Si possible, envisagez d'utiliser un ensemble commun d'outils d'orchestration et de déploiement adaptés aux différentes ressources des fournisseurs de cloud. Cela offre une plus grande flexibilité et simplifie les opérations sur plusieurs clouds. Cependant, il peut être plus simple d'utiliser l'automatisation native de chaque fournisseur séparément et d'établir des processus organisationnels pour garantir une utilisation appropriée.
- Avez-vous des exigences réglementaires et de conformité auxquelles chaque fournisseur de cloud doit satisfaire ?

Vous pouvez avoir des considérations réglementaires qui dictent la manière dont les données doivent être stockées et traitées. Concentrez-vous sur la normalisation des politiques (telles que le trafic réseau, le stockage et la sécurité) qui peuvent être appliquées automatiquement à chaque environnement cloud par l'intermédiaire des fournisseurs de cloud. Réfléchissez à la manière dont vos applications communiqueront avec leurs données et hébergez-les chez le même fournisseur. Si vos applications et leurs données sont fragmentées entre les fournisseurs, il sera difficile de garantir que vous respectez les exigences réglementaires et de conformité. Il est souvent préférable d'avoir des applications aussi proches que possible des données afin de minimiser la latence du réseau, d'optimiser le débit de données et de limiter les sorties de données tout en simplifiant les contrôles de sécurité et d'accès.

- Êtes-vous en mesure de minimiser le coût total de possession et de maximiser les remises lorsque vous déployez des applications auprès de fournisseurs de cloud ?

  Il est important de prendre en compte le coût total de possession (TCO) lorsque l'on envisage le multicloud. L'exécution de vos applications sur plusieurs fournisseurs de cloud peut augmenter les coûts opérationnels et les frais administratifs liés à la maintenance et à la gestion des ressources dans chaque environnement. En outre, en répartissant l'utilisation entre plusieurs fournisseurs, il est plus difficile de tirer parti des remises sur les prix de volume ou des accords d'entreprise d'un fournisseur spécifique. Tenez compte de ces facteurs lorsque vous déterminez si les avantages du multicloud justifient l'augmentation du coût total de possession.

Exemples de cas d’utilisation

Pour mieux comprendre l'application de ces principes dans différents scénarios, examinons quelques exemples de cas d'utilisation. Ces cas d'utilisation sont basés sur la manière dont les établissements d'enseignement du monde réel adoptent les services cloud.

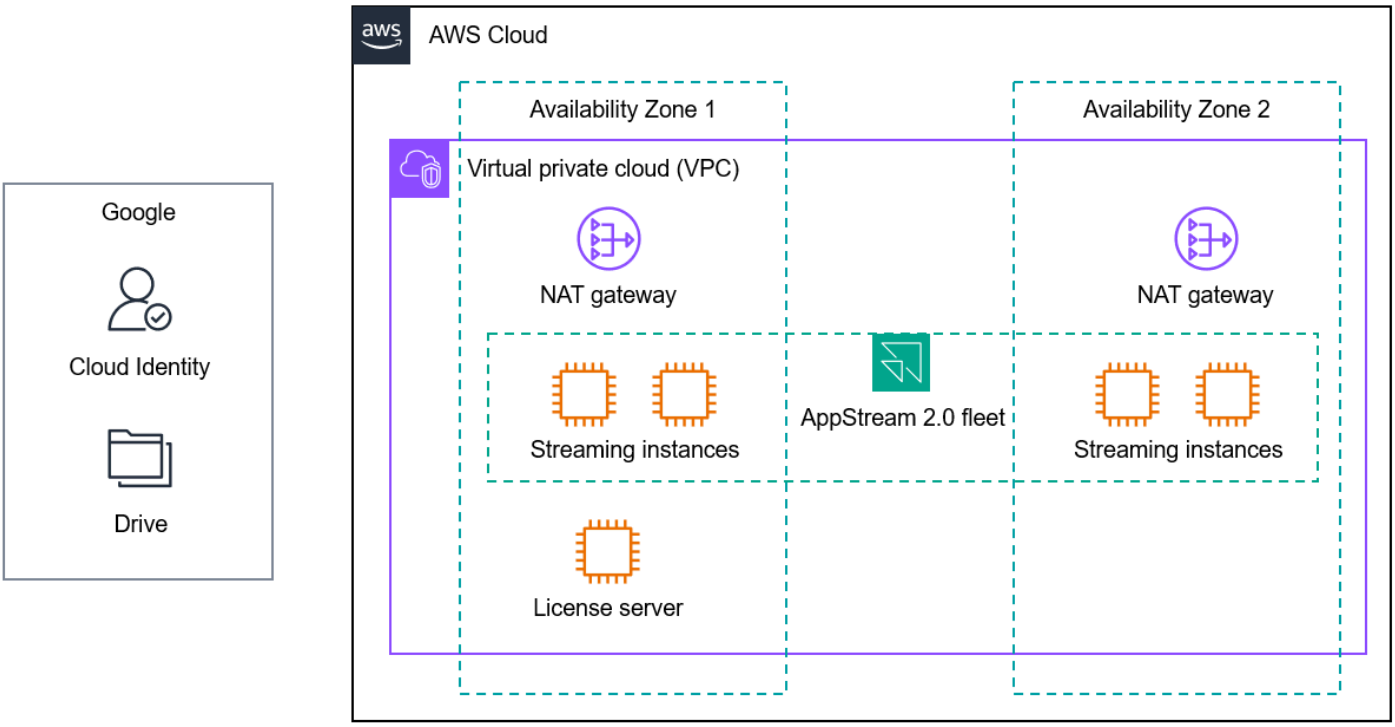
- Laboratoires informatiques virtuels
- Prédire la réussite des élèves
- Fédération d'identité et authentification unique
- L'explosion du cloud pour l'informatique de recherche

Laboratoires informatiques virtuels

Malgré la popularité des outils d'apprentissage basés sur le Web et l'abondance d'appareils utilisateur tels que les ordinateurs portables, les Chromebooks et les tablettes, la plupart des établissements d'enseignement disposent de laboratoires informatiques physiques pour les applications gourmandes en ressources ou anciennes. Ces laboratoires informatiques sont souvent indispensables pour les sciences, la technologie, l'ingénierie et les mathématiques (STEM), l'enseignement professionnel et technique (CTE), les médias et les arts, l'ingénierie et les programmes similaires. Les écoles peuvent augmenter ou remplacer les laboratoires informatiques physiques par des bureaux virtuels basés sur le cloud ou des services de streaming d'applications afin de garantir que tous les élèves ont accès aux applications dont ils ont besoin à tout moment, en tout lieu et sur n'importe quel appareil. Cela améliore l'équité numérique, permet l'apprentissage à distance, garantit une expérience utilisateur cohérente et sécurise l'accès à distance tout en réduisant les coûts.

Dans l'enseignement primaire et secondaire (K-12), de nombreuses écoles américaines utilisent Amazon WorkSpaces Applications, un service de streaming d'applications et de postes de travail entièrement géré, pour proposer des laboratoires informatiques virtuels donnant accès à Adobe Creative Cloud, aux logiciels Autodesk, aux programmes STEM et CTE tels que Project Lead the Way (PLTW), etc. De nombreuses organisations de l'enseignement primaire et secondaire gèrent déjà l'authentification unique des étudiants et le stockage de fichiers via Google Workspace et Google Drive, qui sont des applications SaaS. Ces institutions peuvent configurer l'authentification unique entre Google Workspace et WorkSpaces Applications via la fédération SAML 2.0. Ils peuvent également configurer l'intégration native entre les WorkSpaces applications et Google Drive afin

que les étudiants puissent utiliser le stockage existant. Le schéma suivant illustre le déploiement WorkSpaces des applications pour ce cas d'utilisation.



Cette architecture suit les recommandations suivantes :

- Sélectionnez un fournisseur de cloud principal et stratégique.Cette architecture utilise les services cloud d'un fournisseur de cloud principal. Bien qu'elle inclue l'intégration avec des applications SaaS qui ne sont pas hébergées chez le même fournisseur, ces intégrations se font par le biais de configurations simples. L'expertise et les compétences du cloud ne sont nécessaires que pour déployer et gérer les services du fournisseur de cloud principal.
- Faites la différence entre les applications SaaS et les services cloud de base.Google Workspace et Google Drive ne sont pas hébergés sur le même fournisseur de cloud que la AppStream version 2.0, mais cela est acceptable car ce déploiement fournit les intégrations nécessaires. L'authentification unique permet une gestion centralisée des identités et est configurée de manière sécurisée via SAML 2.0. L'activation du stockage permanent dans le cloud pour les étudiants nécessite de simples modifications de configuration dans Google Drive et dans WorkSpaces les applications.
- Définissez les exigences de sécurité et de gouvernance pour chaque fournisseur de services cloud.Les services et les intégrations utilisés dans cette architecture permettent de répondre aux exigences de sécurité et de gouvernance d'une institution. Le trafic de streaming est crypté. La

fédération via Google Workspace permet de centraliser la gestion des identités. Les services réseau tels qu'Amazon Virtual Private Cloud (Amazon VPC) prennent en charge la configuration des sous-réseaux, du routage et des pare-feux. Vous pouvez filtrer le contenu à l'aide de la configuration DNS, d'agents, d'appareils virtuels ou de services gérés tels que le pare-feu Amazon Route 53 Resolver DNS. Vous pouvez utiliser des services tels que AWS Control Towerpour vous assurer que le compte AWS hébergeant WorkSpaces les applications respecte les règles et contrôles organisationnels standard.

- Adoptez des solutions gérées natives pour le cloud chaque fois que cela est possible et pratique. WorkSpaces Applications est un service géré pour le streaming d'applications et de postes de travail. Vous pouvez diffuser des postes de travail et des applications sans vous soucier du provisionnement, du dimensionnement ou de la maintenance des serveurs. Vous installez vos applications, vous connectez les solutions d'identité, de réseau et de stockage appropriées, puis vous gérez et diffusez ces applications de manière centralisée à vos utilisateurs. Cela élimine une grande partie de la charge de travail indifférenciée qui serait nécessaire pour gérer votre propre solution de streaming de bureau virtuel.

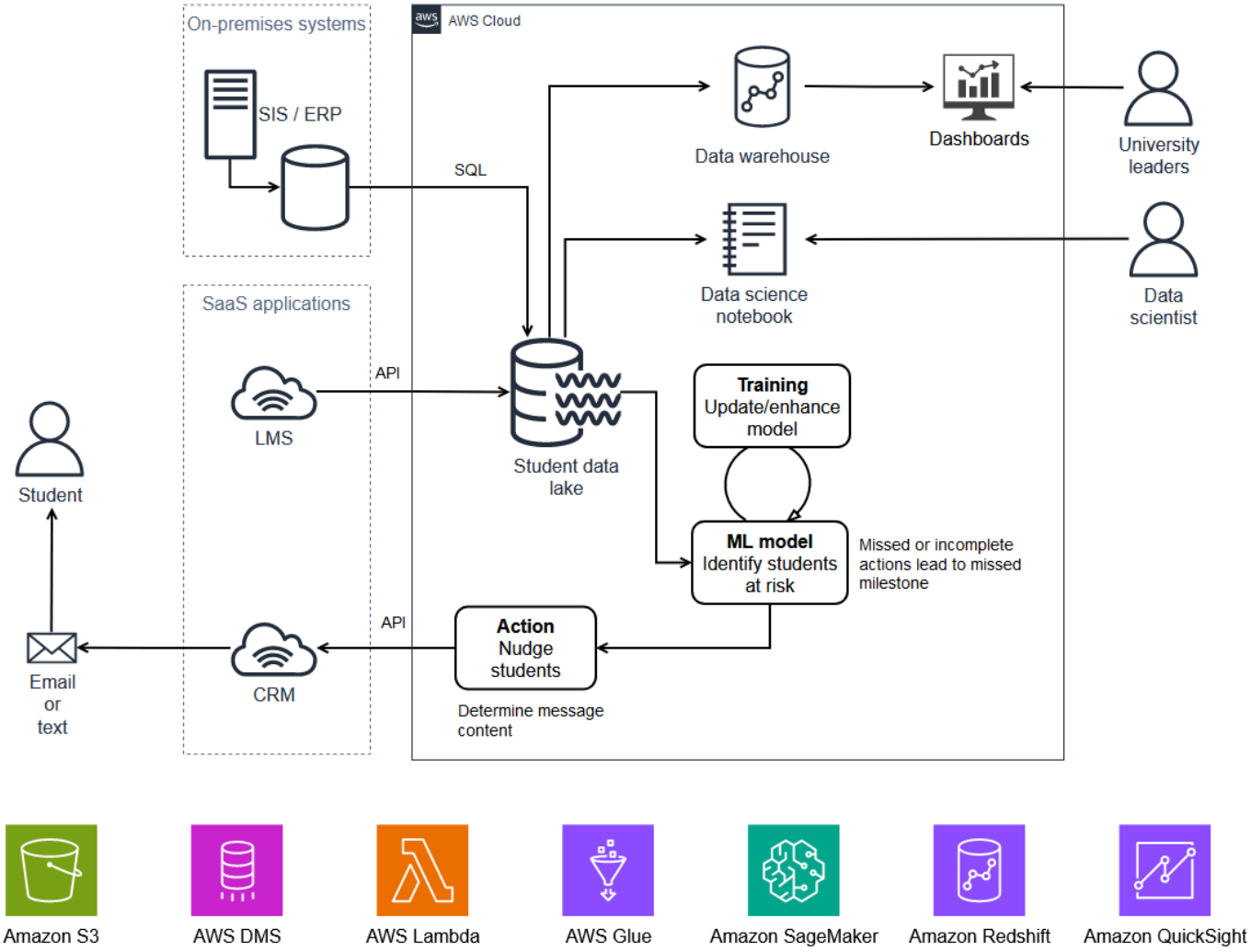
Prédire la réussite des élèves

Une université du Midwest américain a découvert qu'une poignée d'activités clés pour les nouveaux étudiants de première année étaient hautement prédictives de réussite, à la fois pendant le premier semestre de cours de l'étudiant et lors de l'obtention de son diplôme. L'université souhaitait mettre en place un système permettant de surveiller l'achèvement de ces activités et, lorsque les échéances clés approchaient ou étaient dépassées, elle souhaitait encourager les étudiants à suivre ces étapes.

Les données du système de gestion de l'apprentissage (LMS) SaaS ont joué un rôle clé dans cette solution, mais il s'est avéré difficile d'y accéder et de les traiter avec les outils d'entreposage de données de l'équipe informatique de l'université. En outre, les messages destinés aux étudiants devaient être envoyés via le système de gestion de la relation client (CRM) basé sur le cloud de l'école. Pour créer une solution fonctionnelle et évaluer l'efficacité des instructions adressées aux étudiants, l'université a dû lancer des messages via le CRM et en recueillir des données.

L'université a développé et déployé une solution dans un environnement cloud unique. La solution est un mélange de services gérés natifs dans le cloud, de serveurs cloud provisionnés et d'intégrations avec des systèmes sur site et des applications SaaS basées sur le cloud. Comme le montre le schéma suivant, la solution intègre les données du système d'information des étudiants (SIS), du LMS et du CRM dans un lac de données. Il utilise ces données pour identifier les étudiants qui

risquent de manquer des activités clés, leur envoie des messages via le CRM et fournit un tableau de bord à la direction de l'université.



Cette architecture suit les recommandations suivantes :

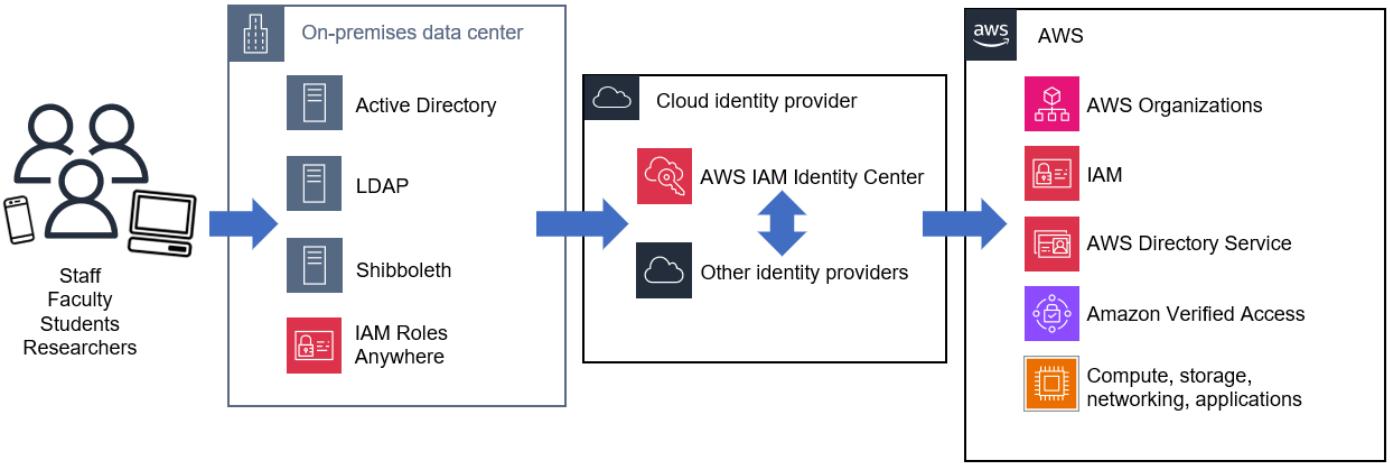
- Sélectionnez un fournisseur de cloud principal et stratégique.Le fournisseur de cloud stratégique de l'université héberge l'intégralité de la solution déployée. Cela permet au personnel informatique et commercial de se concentrer sur le développement des compétences dans un ensemble unique et intégré de fonctionnalités cloud.
- Faites la différence entre les applications SaaS et les services cloud de base.L'université fait la différence entre les applications SaaS et les principaux services d'analyse dans le cloud, et utilise des intégrations avec les applications SaaS pour collecter des données et initier les communications appropriées.

- Définissez les exigences de sécurité et de gouvernance pour chaque fournisseur de services cloud.L'université veille à ce que tous les composants de l'architecture soient sécurisés en appliquant des garde-fous et des contrôles, y compris le chiffrement en transit et au repos, afin de gérer les données des étudiants de manière appropriée.
- Adoptez des solutions gérées natives pour le cloud chaque fois que cela est possible et pratique.Les services gérés natifs dans le cloud sont utilisés pour les fonctionnalités d'ingestion, de stockage, de base de données et d'extraction, de transformation et de chargement (ETL), ce qui réduit le temps de développement du flux de travail de traitement end-to-end des données.

Fédération d'identité et authentification unique

Garantir une gestion cohérente des identités sur l'ensemble des systèmes principaux est essentiel pour adopter une technologie avec succès et en toute sécurité. Les établissements d'enseignement adoptent de plus en plus des solutions d'identité et d'authentification unique basées sur le cloud AWS IAM Identity Center, telles que Microsoft Entra ID (anciennement Azure Active Directory), Okta,, Ping Identity JumpCloud OneLogin, CyberArk afin de simplifier la gestion des identités, de réduire la charge opérationnelle et d'appliquer de manière centralisée les meilleures pratiques telles que l'authentification multifactorielle et l'accès au moindre privilège.

Nombre de ces institutions maintiennent toujours des services de gestion des identités et d'annuaire tels qu'Active Directory et Shibboleth pour leurs environnements sur site. Elles peuvent être intégrées à des solutions basées sur le cloud pour permettre une gestion centralisée des identités et une authentification unique pour vos étudiants, vos professeurs et votre personnel. Les fournisseurs de solutions cloud doivent disposer de plateformes de gestion des easy-to-integrate identités robustes qui vous permettent de fédérer les identités via des fournisseurs d'identité cloud avec vos applications existantes, vos solutions SaaS et vos services cloud. Le schéma suivant montre un exemple d'architecture.



Cette architecture suit les recommandations suivantes :

- Sélectionnez un fournisseur de cloud principal et stratégique.Cette architecture est utilisée AWS comme principal fournisseur de cloud. En s'intégrant à un fournisseur d'identité dans le cloud et aux services de gestion des identités et d'annuaire existants sur site, cette architecture prend en charge le provisionnement et la gestion automatisés de l'accès à la fois aux services du fournisseur de cloud principal et aux autres applications et solutions SaaS. Cela garantit que les exigences de sécurité et de gouvernance sont satisfaites de manière cohérente et facile à gérer à mesure que de nouvelles applications et services sont ajoutés au portefeuille technologique de l'établissement.
- Faites la différence entre les applications SaaS et les services cloud de base.Cette architecture intègre plusieurs types de systèmes d'identité basés sur le cloud, SaaS et sur site pour fournir un accès aux AWS Cloud services et autres applications. De nombreux fournisseurs d'identité et solutions d'authentification unique basés sur le cloud sont également des applications SaaS, et ils peuvent utiliser des intégrations natives et des protocoles standard tels que le SAML pour fonctionner dans différents environnements.
- Définissez les exigences de sécurité et de gouvernance pour chaque fournisseur de services cloud.Cette architecture est conforme aux directives sur la gestion des identités et des accès publiées par de nombreux cadres de sécurité, notamment le cadre de cybersécurité (CSF) du National Institute of Standards and Technology (NIST), le NIST 800-171 et le NIST 800-53. Les intégrations avec AWS Organizations, Gestion des identités et des accès AWS (IAM) et d'autres services de AWS sécurité, d'identité et de conformité permettent de fournir des contrôles d'accès sécurisés et granulaires basés sur les autorisations de groupe.
- Adoptez des services gérés natifs dans le cloud chaque fois que cela est possible et pratique.Cette architecture utilise des services gérés basés sur le cloud pour la gestion des identités et

l'authentification unique. Cela réduit le temps et l'énergie consacrés à la gestion des infrastructures et facilite la maintenance de ces systèmes critiques.

- Mettez en œuvre des architectures hybrides lorsque les investissements existants sur site incitent à une utilisation continue.Cette architecture intègre les investissements existants sur site dans l'infrastructure d'hébergement des charges de travail Active Directory, Lightweight Directory Access Control (LDAP) et Shibboleth, et fournit un moyen de transférer à terme les principaux services d'identité vers une infrastructure basée sur le cloud. En outre, si vos charges de travail sur site nécessitent un accès aux AWS ressources basé sur des certificats, vous pouvez utiliser Roles Anywhere.Gestion des identités et des accès AWS

L'explosion du cloud pour l'informatique de recherche

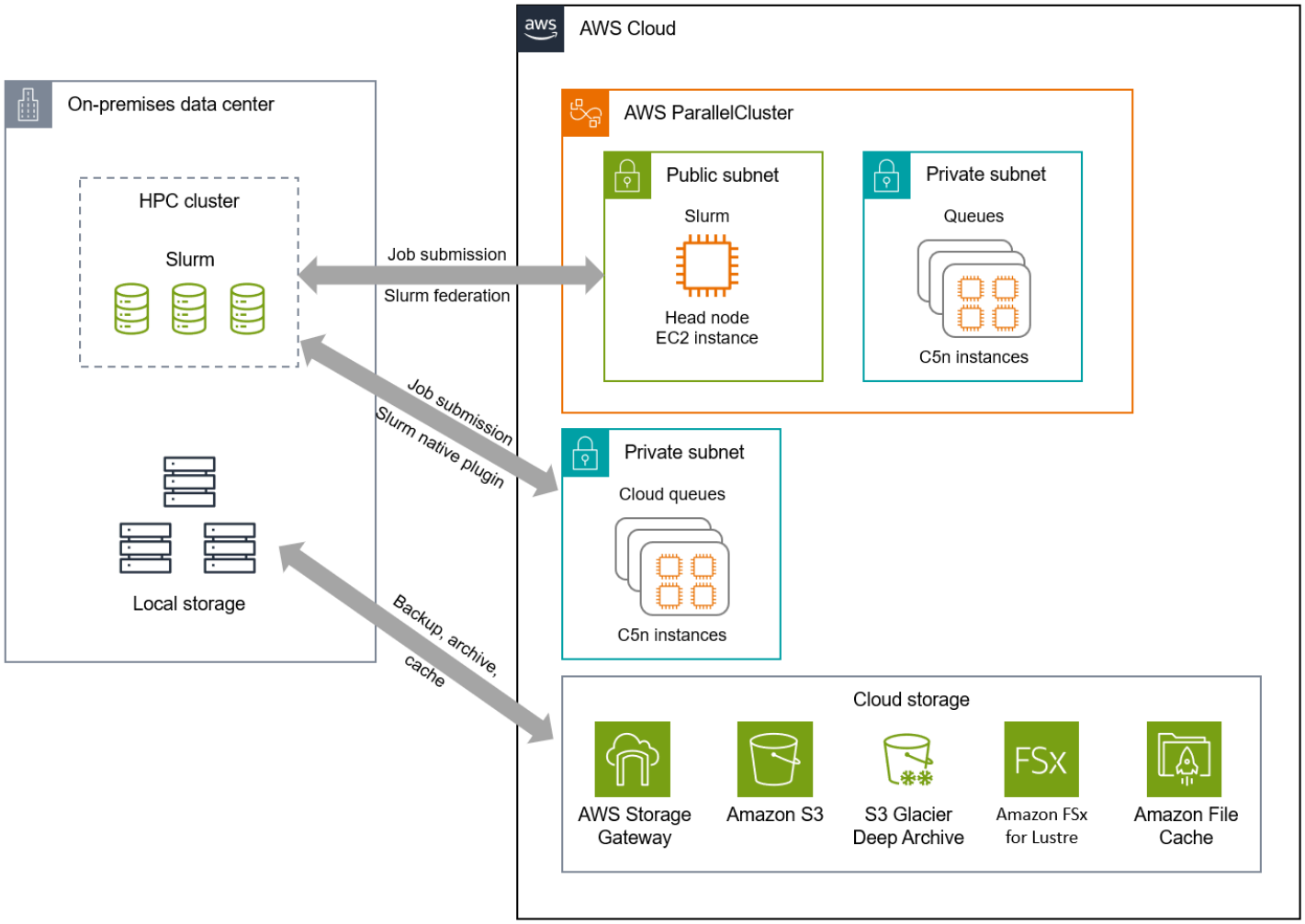
Le groupe informatique de recherche d'une institution de recherche R1 (Doctoral Universities — Very High Research Activity) aux États-Unis gérait des clusters de calcul haute performance (HPC) sur site avec le planificateur Slurm depuis de nombreuses années. À l'exception de quelques semaines de maintenance planifiée, les clusters fonctionnaient à un taux d'utilisation de 80 à 95 % et la plupart de leurs files d'attente étaient pleines.

Le nombre croissant d'activités de recherche au sein de l'établissement a posé des problèmes de capacité et de capacité. Quelques chercheurs de renom effectuaient toujours des simulations de longue durée sur certaines files d'attente, ce qui augmentait le temps d'attente pour les autres utilisateurs. Les professeurs nouvellement embauchés devaient exécuter un grand nombre de simulations météorologiques pour créer un nouveau modèle d'intelligence artificielle et d'apprentissage automatique (AI/ML) pour les prévisions météorologiques, mais ils nécessitaient une capacité supérieure à celle disponible. Le groupe informatique de recherche recevait également de plus en plus de demandes concernant les dernières unités de traitement graphique (GPUs) destinées à entraîner des modèles d'apprentissage automatique. Même avec un financement pour de nouvelles installations GPUs, l'équipe devra attendre des mois avant d'obtenir l'autorisation d'agrandir l'espace rack du centre de données.

De nombreux chercheurs n'étaient pas disposés à supprimer les anciennes données, de sorte que la capacité de stockage locale représentait également un défi. Une option de stockage à long terme plus évolutive était nécessaire pour libérer du stockage précieux et performant sur site.

Le cloud répond à ces défis grâce à des solutions hybrides de calcul et de stockage qui vous permettent d'intégrer le calcul de recherche dans le cloud lorsque la capacité sur site ne suffit pas. Le

schéma d'architecture suivant illustre quelques approches de calcul et de stockage en rafale, à l'aide d'outils tels que AWS ParallelClusteret AWS Storage Gateway.



Cette architecture suit les recommandations suivantes :

- Sélectionnez un fournisseur de cloud principal et stratégique.Cette architecture utilise un fournisseur de cloud principal pour éviter d'être limitée par l'approche du plus petit dénominateur commun. Ainsi, l'établissement peut tirer parti de l'innovation et des services de calcul et de stockage natifs proposés par le principal fournisseur de cloud. L'équipe informatique de recherche peut se concentrer sur l'optimisation des charges de travail dans l'environnement fourni par le fournisseur de cloud principal, et non sur la manière de travailler dans différents environnements cloud.
- Définissez les exigences de sécurité et de gouvernance pour chaque fournisseur de services cloud.Chaque service et outil utilisé dans cette architecture peut être configuré pour répondre aux exigences de sécurité et de gouvernance de l'équipe informatique de recherche, notamment

la connectivité privée, le chiffrement des données en transit et au repos, l'enregistrement des activités, etc.

- Adoptez des services gérés natifs dans le cloud chaque fois que cela est possible et pratique.Cette architecture permet d'utiliser des services de stockage et de calcul gérés ainsi que des outils pour simplifier la gestion des clusters. Ainsi, l'équipe informatique de recherche n'a pas à se soucier de gérer elle-même les clusters ou l'infrastructure sous-jacente, ce qui peut s'avérer complexe et chronophage.
- Mettez en œuvre des architectures hybrides lorsque les investissements existants sur site incitent à une utilisation continue.Cette architecture permet à l'établissement de continuer à utiliser ses ressources sur site et de tirer parti du cloud pour augmenter sa capacité et sa puissance de calcul à la demande. Grâce au cloud, l'établissement peut ajuster le type de calcul pour optimiser le rapport prix/performances et accéder aux dernières technologies afin de promouvoir l'innovation sans un investissement initial important dans du matériel supplémentaire sur site.

Étapes suivantes

La sélection du modèle de déploiement adapté aux charges de travail dans le cloud nécessite un examen attentif. Utilisez les recommandations présentées dans ce paper pour guider votre prise de décision et éviter les écueils courants tels que la complexité inutile, l'augmentation des exigences du personnel, les incohérences dans la gouvernance et les approches fondées sur le plus petit dénominateur commun. En suivant ces bonnes pratiques, vous pouvez accélérer votre adoption du cloud pour atteindre et dépasser les objectifs de votre établissement de manière plus efficace.

N'oubliez pas de sélectionner un fournisseur de cloud stratégique principal et de créer un centre d'excellence cloud (CCoE) pour favoriser la maturité organisationnelle et garantir votre succès à long terme. Faites la différence entre les applications SaaS et les services cloud de base, et identifiez les principales exigences de sécurité et de gouvernance pour chacun d'entre eux. Dans la mesure du possible, adoptez des services gérés natifs pour le cloud et implémentez des architectures hybrides lorsque les investissements dans vos centres de données existants encouragent une utilisation continue. Enfin, réservez le multicloud uniquement aux charges de travail qui en ont réellement besoin.

AWS est bien placé pour vous aider à gérer des environnements monocloud, hybrides et multicloud. Votre établissement peut utiliser AWS des solutions de gestion et d'observabilité telles que AWS Systems ManagerAWS Config, et Amazon CloudWatch pour simplifier et centraliser la gestion et la surveillance de votre infrastructure et de vos applications, quel que soit votre environnement. Avec des services de données et d'analyse tels qu'Amazon Athena et AWS GlueAWS DataSync, vous pouvez obtenir des informations à partir de toutes vos données, où qu'elles soient stockées. Les solutions hybrides telles que AWS OutpostsAWS Wavelength, et vous AWS Snow Familypermettent d'apporter AWS l'infrastructure et les services là où ils sont nécessaires. Des outils tels qu'Amazon EKS Distro vous aident à créer des clusters Kubernetes autogérés sur AWS, sur site ou sur d'autres clouds.

Lorsque vous définissez votre stratégie cloud, considérez les étapes suivantes :

1. Passez en revue le cadre d'adoption du AWS cloud (AWS CAF) pour identifier et hiérarchiser les opportunités de transformation, évaluer et améliorer votre préparation au cloud et faire évoluer de manière itérative votre feuille de route de transformation.
2. Identifiez un système pour la mise en œuvre du cloud pour commencer comme preuve de concept. Cela vous aidera à définir la base ou le cadre du cloud pour valider toutes les hypothèses, et permettra également les futures implémentations du cloud.

3. Demandez à l'équipe chargée de votre AWS compte de discuter de vos objectifs de mise en œuvre du cloud. L'équipe chargée du AWS compte peut vous aider à apporter des clarifications, à suggérer des approches, à identifier les dépendances et à travailler avec vos équipes pour planifier votre parcours, du concept initial à la mise en œuvre.

Collaborateurs

Les contributeurs à ce guide incluent :

- Kevin Arand, directeur principal de l'architecture des solutions, de l'enseignement, AWS
- Kevin McCandless, architecte de solutions senior, enseignement de la maternelle à la 12e année, AWS
- Craig Jordan, architecte de solutions principal, enseignement, AWS
- Jesse Roberts, architecte de solutions principal, SLG et K-12 Education, AWS
- Jianjun Xu, architecte de solutions principal, enseignement, AWS
- Josh Badal, architecte de solutions senior, enseignement, AWS
- Raj Chary, architecte de solutions senior, enseignement, AWS

Suggestions de lecture

Pour en savoir plus, reportez-vous à :

- AWS Centre d'architecture
- Transformation du cloud dans le secteur public
- AWS Cadre d'adoption du cloud (AWS CAF)
- AWS Solutions pour le cloud hybride et multicloud

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	—	15 septembre 2023

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 sur site vers Oracle sur une instance EC2 dans le. AWS Cloud
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers AWS.
- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

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

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

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

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

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

Consultez la base de données de gestion des configurations.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

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

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

administrateur délégué

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

déploiement

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

environnement de développement

Voir environnement.

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

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

reprise après sinistre (DR)

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

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

DR

Voir reprise après sinistre.

détection de dérive

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

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

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

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

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 CSPM GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation des historiens

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

données de rétention

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l’identité

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

application inactive

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

IIo T

Voir Internet industriel des objets.

infrastructure immuable

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

VPC entrant (d'entrée)

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

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

migration incrémentielle

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

Industry 4.0

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 lorsqu'il fonctionne. Pour plus d'informations, voir Création de mécanismes dans le cadre AWS Well-Architected.

compte membre

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

MAILLES

Voir le système d'exécution de la fabrication.

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

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

microservice

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

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

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

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés peuvent accéder au contenu d'un compartiment S3 uniquement via 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.

policy

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

persistance polyglotte

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

Entité AWS capable d'effectuer des actions et d'accéder aux ressources. Cette entité est généralement un utilisateur root pour un Compte AWS rôle IAM ou un utilisateur. Pour plus

d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

confidentialité dès la conception

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

zones hébergées privées

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

contrôle proactif

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

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

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

RAG

Voir Retrieval Augmented Generation.

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Région

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

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération (RAG)

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

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de temps de rétablissement.

runbook

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

S

SAML 2.0

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

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

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

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

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

Politique qui 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, voir 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

tags

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.

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.